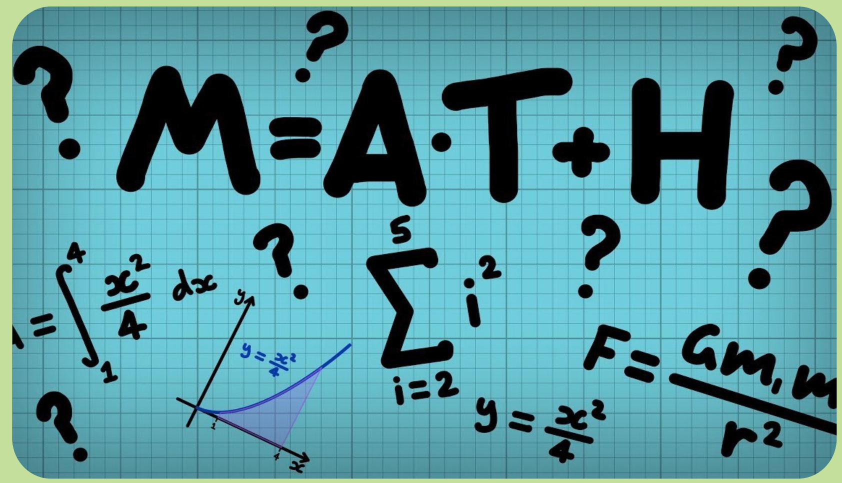
Science Faculty

Afghanic

Dr Abdullah Momand

Algebra (in pashto)



ISBN 978-9936-620-67-4

Funded by
inasys GmbH Germany

Not for Sale

2019

معاصر الجبر

Algebra (in Pashto)

داکتر عبدالله مهمند

ساينس پوهنځي

معاصر الجبر

$$(a+b)^2 = a^2 + b^2 \, (a, b \in (Z_2^*, .)$$

$$(a+b)^2 = a^2 + 2ab + b^2 \, (a\ b \in R^*, .)$$

داکتر عبدالله مهمند

پلورل منع دي

۱۳۹۸

بسم الله الرحمن الرحيم

معاصر الجبر

داکتر عبدالله مهمند

لومړی چاپ، ۲۰۱۹

د کتاب نوم معاصر الجبر
لیکوال داکتر عبدالله مهمند
خپرندوی شیخ زاید پوهنتون، ساینس پوهنځی
وېب پاڼه www.szu.edu.af
د چاپ کال ۱۳۹۸، لومړی چاپ
چاپ شمېر ۱۰۰۰
مسلسل نمبر ۲۹۳
ډاونلوډ www.ecampus-afghanistan.org
چاپ ځای سهر مطبعه، کابل، افغانستان

دا کتاب په آلمان کې د اناسیس کمپنۍ په مرسته چاپ او د کتاب اداري او تخنیکي چارې په آلمان کې د افغانیک لخوا ترسره شوي دي.
د کتاب د محتوا او لیکنې مسئولیت د کتاب په لیکوال او اړونده پوهنځي پورې اړه لري. مرسته کوونکي او تطبیق کوونکې ټولنې په دې اړه مسؤلیت نه لري.

د تدریسي کتابونو د چاپولو لپاره له موږ سره اړیکه ونیسئ:
ډاکتر یحیی وردک، د لوړو زده کړو وزارت، کابل
ټېلیفون ۰۷۰۶۳۲۰۸۴۴، ۰۷۵۶۰۱٤٦۴۰
ایمېل textbooks@afghanic.de

ای اس بي ان ۹۷۸-۹۹۳٦-٦۲۰-٦۷-۴

د لوړو زده کړو وزارت پیغام

د بشر په مختلفو دورو کې کتاب د علم او پوهې په لاسته راوړلو، ساتلو او خپرولو کې ډیر مهم رول لوبولی دی. درسي کتاب د نصاب اساسي برخه جوړوي چې د زده کړې د کیفیت په لوړولو کې مهم ارزښت لري. له همدې امله د نړیوالو پیژندل شویو معیارونو، د وخت د غوښتنو او د ټولنې د اړتیاوو په نظر کې نیولو سره باید نوي درسي مواد او کتابونه د محصلینو لپاره برابر او چاپ شي.

له ښاغلو استادانو او لیکوالانو څخه د زړه له کومي مننه کوم چې دوامداره زیار یې ایستلی او د کلونو په اوږدو کې یې په خپلو اړوندو څانگو کې درسي کتابونه تألیف او ژباړلي دي، خپل ملي پور یې اداء کړی دی او د پوهې موتور یې په حرکت راوستی دی. له نورو ښاغلو استادانو او پوهانو څخه هم په درنښت غوښتنه کوم تر څو په خپلو اړوندو برخو کې نوي درسي کتابونه او درسي مواد برابر ، چې له چاپ وروسته د گرانو محصلینو په واک کې ورکړل شي او د زده کړو د کیفیت په لوړولو او د علمي پروسې په پرمختگ کې یې نېک گام اخیستی وي.

د لوړو زده کړو وزارت دا خپله دنده بولي چې د گرانو محصلینو د علمي سطحې د لوړولو لپاره د علومو په مختلفو رشتو کې معیاري او نوي درسي مواد برابر او چاپ کړي.

په پای کې زموږ د همکار ډاکتر یحیی وردک څخه مننه کوم چې د دی کتاب د خپرولو لپاره یې زمینه برابره کړېده.

هیله مند یم چې د درسي کتابونو د چاپولو گټوره پروسه دوام وکړي او پراختیا ومومي تر څو په نیږدې راتلونکې کې د هر درسي مضمون لپاره لږ تر لږه یو معیاري درسي کتاب ولرو.

په درنښت

پوهنمل دیپلوم انجنیر عبدالتواب بالاکرزی

د لوړو زده کړو علمي معین او سرپرست وزیر

کابل، ۱۳۹۸

د درسي کتابونو چاپول

قدرمنو استادانو او ګرانو محصلینو!

د افغانستان په پوهنتونونو کې د درسي کتابونو کموالی او نشتوالی له لویو ستونزو څخه ګڼل کېږي. یو زیات شمیر استادان او محصلین نویو معلوماتو ته لاس رسی نه لري، په زاړه میتود تدریس کوي او له هغو کتابونو او چپترونو څخه ګټه اخلي چې زاړه دي او په بازار کې په ټیټ کیفیت فوتوکاپي کېږي.

تر اوسه پورې موږ د ننګرهار، خوست، کندهار، هرات، بلخ، البیروني، کابل، کابل طبي پوهنتون او کابل پولي تخنیک پوهنتون لپاره څه کم ۳۰۰ عنوانه مختلف درسي کتابونه د طب، ساینس، انجنیري، اقتصاد، ژورنالیزم او زراعت پوهنځیو (۹٦ طبي د آلمان د علمي همکاریو ټولنې DAAD، ۱۷۰ طبي او غیر طبي د افغان ماشومانو لپاره د جرمني کمېټې Kinderhilfe-Afghanistan، ۷ کتابونه د آلماني او افغاني پوهنتونونو ټولنې DAUG، ۲ کتابونه په مزار شریف کې د آلمان فدرال جمهوري جنرال کنسولګري، ۳ کتابونه د Afghanistan-Schulen، ۱ د صافی بنسټ لخوا، ۲ د سلواک اېډ او ۸ نور کتابونه د کانراد ادناور بنسټ KAS) په مالي مرسته چاپ کړي دي.

د یادونې وړ ده، چې نوموړي چاپ شوي کتابونه د هېواد ټولو اړونده پوهنتونونو او یو زیات شمېر ادارو او مؤسساتو ته په وړیا توګه وېشل شوي دي.

ټول چاپ شوي کتابونه له www.afghanistan-ecampus.org ویب پاڼې څخه ډاونلوډ کولای شئ.

دا کړنې په داسې حال کې تر سره کېږي چې د افغانستان د لوړو زده کړو وزارت د (۲۰۱۰ - ۲۰۱۴) کلونو په ملي ستراتیژیک پلان کې راغلي دي چې:

"د لوړو زده کړو او د ښوونې د ښه کیفیت او زده کوونکو ته د نویو، کره او علمي معلوماتو د برابرولو لپاره اړینه ده چې په دري او پښتو ژبو د درسي کتابونو د لیکلو فرصت برابر شي د تعلیمي نصاب د ریفورم لپاره له انګریزي ژبې څخه دري او پښتو ژبو ته د کتابونو او درسي موادو ژباړل اړین دي، له دې امکاناتو څخه پرته د پوهنتونونو محصلین او استادان نشي کولای عصري، نویو، تازه او کره معلوماتو ته لاس رسی پیدا کړي."

موږ غواړو چې د درسي کتابونو په برابرولو سره د هیواد له پوهنتونونو سره مرسته وکړو او د چپټر او لکچر نوټ دوران ته د پای ټکی کېږدو. د دې لپاره دا اړینه ده چې د لوړو زده کړو د موسساتو لپاره هر کال څه نا څه ۱۰۰ عنوانه درسي کتابونه چاپ شي.

له ټولو محترمو استادانو څخه هیله کوو، چې په خپلو مسلکي برخو کې نوي کتابونه ولیکي، وژباړي او یا هم خپل پخواني لیکل شوي کتابونه، لکچر نوټونه او چپټرونه ایډېټ او د چاپ لپاره تیار کړي، زمونږ په واک کې یې راکړي چې په ښه کیفیت چاپ او وروسته یې د اړوند پوهنځیو، استادانو او محصلینو په واک کې ورکړو. همدارنګه د یاد شویو ټکو په اړوند خپل وړاندیزونه او نظریات له مونږ سره شریک کړي، تر څو په ګډه پدې برخه کې اغېزمن ګامونه پورته کړو.

د مؤلفینو او خپروونکو له خوا پوره زیار ایستل شوی دی، ترڅو د کتابونو محتویات د نړیوالو علمي معیارونو په اساس برابر شي، خو بیا هم کیدای شي د کتاب په محتوا کې ځینې تیروتنې او ستونزې ولیدل شي، نو له درنو لوستونکو څخه هیله مند یو تر څو خپل نظریات او نیوکې مؤلف او یا مونږ ته په لیکلې بڼه راولیږي، تر څو په راتلونکي چاپ کې اصلاح شي.

د اناسیس د کمپنۍ څخه ډېره مننه کوو چې د دغه کتاب د چاپ لګښت یې ورکړی دی.

او د جي آی زیت (GIZ) له دفتر او CIM (Center for International Migration & Development) څخه، چې زما لپاره یې له ۲۰۱۰ نه تر ۲۰۱٦ پورې په افغانستان کې د کار امکانات برابر کړي وو، هم د زړه له کومې مننه کوم.

د لوړو زده کړو له سرپرست وزیر پوهنمل دیپلوم انجنیر عبدالتواب بالاکرزی، مالي او اداري معین ډاکتر احمد سیر مهجور علمي معین او، مالي او اداري رئیس احمد طارق صدیقي، په لوړو زده کړو وزارت کې سلاکار ډاکتر ګل رحیم صافي، د پوهنتونونو رئیسانو، د پوهنځیو رییسانو او استادانو څخه مننه کوم چې د کتابونو د چاپ لړۍ یې هڅولې او مرسته یې ورسره کړې ده. د دغه کتاب له مؤلف څخه ډېر منندوی یم او ستاینه یې کوم، چې خپل د کلونو-کلونو زیار یې په وړیا توګه ګرانو محصلینو ته وړاندې کړ.

همدارنګه د دفتر له همکارانو هر یو حکمت الله عزیز او فهیم حبیبي څخه هم مننه کوم چې د کتابونو د چاپ په برخه کې یې نه ستړې کیدونکې هلې ځلې کړې دي.

ډاکتر یحیی وردک، د لوړو زده کړو وزارت سلاکار

کابل، نومبر، ۲۰۱۹

د دفتر ټیلیفون: ۰۷۵٦۰۱۴٦۴۰، ۰۷۰٦۳۲۰۸۴۴

ایمیل: textbooks@afghanic.de

بسم الله الرحمن الرحيم

ځرنګه چې په افغانستان کې دمعاصرالجبرپه برخه کې په پښتواودرى ډيرلږاويا هيڅ ليکني نه دي شوي ، له دې کبله غواړم دلته د الجبر(چې د مدرن الجبر ، مجرد الجبر اويا معاصر الجبر په نوم هم ياديږي) ځني اساسات او مفاهيم چې په الجبرکې ډير عموميت لري اوله هغه څخه په رياضياتوکې زياته استفاده کيږي، دلته وليکم. ځرنګه چې په وخت تيريدوسره کلاسيک عملياتولکه جمع "+" او ضرب "." نشوکولاى ځني مسايل حل کړي. دا سبب شو چې علما د دا ډول موضوعات د حل لپاره نوي عمليات (operation) تعريف کړل. ځرنګه چې N.H. Abel په 1826 کال کې د الجبرى معادلاتو چې درجه يې تر 3 زياته وې د حل لپاره ديوفورمل په پيدا کولو کې بريالى نشو. بيا په هغه وخت کې ديو الجبرى جوړښت (ساختمان) نظر يوې دوه ګوني رابطه (binary operation) ته د تعريف په فکر کې شول او دا البته شروع د معاصر (مدرن) الجبر وه. وروسته بيا د نوروعلماوله خوا لکه D. Hilbert ، E. Steinitz او R.Dedekind مدرن الجبر ته انکشاف ورکړل شو. چې نن هغه په مختلفو څانګود مثال په ډول Group (ګروپ) ، Ring (حلقه) ، Field (ساحه) اونورو تقسيم شوي دي. په دې چاپ کې د ګروپو ، حلقو او ساحو د مفصل تشريح څخه صرف نظر شوى دى . علاوه پرهغه د Cryptography (رمز ليکني) په باره کي معلومات اودهغي استفاده دمعاصرالجبرڅخه د مثالو سره پدي کتاب کي ليکل شويدي. مګرتصميم لرم چې په راتلونکي وخت کې دى ته نورهم وسعت ورکړم. دلته کوښښ شوى دى چې هغه رياضي سمبولونه استعمال شي، چې نن په نړۍ کې په کتابوکې له هغه څخه استفاده کيږي اوتابع د يوي معيني ژبې نه وي. همدارنګه د نومونو په استعمال کې کوښښ شوى دى چې د دو ژبو (پښتو او انګلسى) مروجه نومونو څخه استفاده وشي . البته دا دهغو کسانولپاره چې د رياضى او نورو علمي کتابونه په بين المللي ژبو مطالعه کوي ، د ګټې وړبه هم وي. هغه سمبولونه او اختصارات چې دلته استعمال شوى دي ، په اخيرکې مې تشريح کړى دي.امکان لرى چې په ليکلواو يا د جملاتو په جوړښت کې اشتبهات يا غلطۍ موجودي وي ، معذرت غواړم.

داکتر عبدالله مهمند

د موضوعاتو فهرست

پاتي(باقيماده) كلاسي (residue class)
باقيماده كلاسو گروپ (residue class group)
كيلي قضيه (**Cayley theorem**)

خلورم فصل: Direct product of groups

Direct product of groups
Cartesian product
External direct product
Enternal direct product
Chinese remainder theorem
solve equations of congruent classes

پنځم فصل: دوراني گرووپونه

دورانی گروپونه (cyclic groups)
ایولرفنکشن (Euler function)
prime residue class group

شپږم فصل: رینګ (Ring)

حلقه (Ring)
فرعی رینګ (Subring)
ادیال (ideal)
رینګ هومورفیزم (Ring homomorphism **)**
Prime Ideal
Principle Ideal
رینګ هومورفیزم قضیه (ring homomorphism)
رینګ ایزومورفیزم قضیه (ring isomorphism)
(ناحیه تمامی) Integral domain
Gaussian integers
Euclidean Domain
Characteristic of Ring
پولینوم رینګ (Polynomial Ring**)**
Division Algorithm
Remainder Theorem
(ترټولولمړی مشترک قاسم) greatest common divisor
د پولینوم رینګ

اوم فصل: ساحه

ساحه (Field)
فرعی ساحه (Subfield)

اتم فصل

ساحه يي توسعه (يا امتداد) (Field extensions)

(درجه د ساحه يي توسعي) degree of field extension

الجبری توسعه (Agebraic extension)

لاگرنج قضیه د ساحي لپاره (The theorem of Lagrange for fields)

مینیمال پولینوم (Minimal polynomial)

سپلیتینگ ساحه(Splitting field)

الجبراساسی قضیه (The fundamental theorem of algebra)

کیوسینت ساحه (quotient field)

ایزن شتاین شرطونه د پولینوم لپاره (Eisenstein's criterion)

نـهم فصل

باقیمانده کلاسو معادلات (Equations of congruent classes)

ویتا فورمول (Vieta's formulas)

لسم فصل

کریپتوگرافی (Cryptography)

پولیگ هیلمن کریپتوگرافی سیستم Pohlig-Hellman Cryptsystem

RSA کریپتوگرافی سیستم (RSA-Cryptsystem)

الجمل کریپتوگرافی سیستم (Elgamal-Cryptsystem)

د رياضي اساسات

(مجموعه , انځور(تصوير) او اړيکی (رابطه))

(Set , Mapping and Relation)

پدی فصل کښی غواړم ځنی رياضي اساسات ، مفاهيم اوقضاياوی چې وروسته په معاصر الجبرکې ورځينی استفاده کيږي، په مختصرډول تشريح کړم.

تعريف 0.1: سيت (**set**) د Georg Cantor له خوا په 1874 ميلادي کال کې په لاندې ډول تعريف شوی دی :

Set يوه مجموعه د اوبجيکټونو(Objects) ده چې ټول يو معين مشخصات ولری مګر يوله بل څخه فرق لری. دمثال په ډول که X سيت ساينس د پوهنځی محصلين وی. معين مشخصات دلته دساينس دپوهنځی محصل کيدل دی.

مګر هرمحصل له يوبل څخه فرق لری.مونږ يو سيت په لاندې ډول ښيو:

$$X = \{x_1, x_2, \dots \dots \dots \dots\}$$

دلته $x_1, x_2, x_3 \dots\dots$ Objects دي چې د X د سيت د عناصرو (elements) په نوم يادېږی. ديوه سيت X د عناصروشمير د cardinality په نوم يادېږي اومونږ هغه په $|X|$ سره ښيو. خالی سيت په $\emptyset$ سره ښودل کيږی.

تعريف 0. 2:

(a) که چيری X او Y دوه سيټونه وی. X ته فرعی سيت (subset) د Y ويل کيږی، په دې شرط چې : $(X \subseteq Y)$

$$\forall x \in X \Rightarrow x \in Y$$

يوفرعی سيت X ته (proper subset) د Y ويل کيږي $(X \subset Y)$ ، په دې شرط چې په Y کښی ځنی عناصرموجود وي او په X کې شامل نه وي. يعنې:

$$\exists\, a \in Y\ ;\ a \notin X$$

د مثال په ډول:

X = { 2,4,5}, Y = {2,4,5,a,b}

X يو proper subset د Y دی. ځکه $a, b \notin X$

هرسيت يوخالی فرعی سيت لری. X او Y سره مساوی دی په دې شرط چې $X \subseteq Y$ او $Y \subseteq X$ وي. يعنې:

$$X = Y \;\Leftrightarrow\; (X \subseteq Y) \wedge (Y \subseteq X)$$

(b) دمتناهی سیت (finite set) لپاره ډول ډول تعریفونه موجود دي .
R . Dedekind (1831-1916) متناهی سیت (**finite set**) دارنګه تعریف کړیدی:
یوسیت X ته متناهی ویل کیږي پدی شرط چې په X کښی هیڅ یو پروپر فرعی سیت *(proper subset)* موجود نه وی چې *Cardinality* (دعناصرو شمیر) د X سره مساوی وی . یعنې

$$\nexists\, A \subset X;\; |A| = |X|$$

اویا داچې :

$$\forall\; A \subset X;\; |A| < |X|$$

دلته د متناهی پرځای دمعین او د غیرمتناهی پرځای دغیرمعین کلمه هم استعمالو.
مونږ معین سیت په $X = \{x_1, x_2, \ldots, x_n\}$ سره ښیو. دلته د X دعناصرو شمیر مساوی n دی. یعنې $|X| = n$
هرهغه سیت چې متناهی نه وي دغیرمتناهی سیت (**infinite set**) په نوم یادیږي.
یعنې: $|X| = \infty$
مثال :

$\mathbb{N} = \{\ 1,2,3\ ,3,4, \ldots\}$
$\mathbb{N}_0 = \{\ 0, 1,2,3\ ,3,4, \ldots\}$
$\mathbb{Z} = \{\ldots, -3, -2, -1\ ,0,1,2,3\ , \ldots\}$
$2\mathbb{Z} = \{\ldots, -6, -4, -2\ ,0,2,4,6\ , \ldots\}$
$\mathbb{Q} = \{\frac{p}{q}\ \mid p, q \in \mathbb{Z}, q \neq 0\}$
$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

پورتنی سیتونه ټول غیرمعین (غیرمتناهی) دي . ځکه :

$(\ \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\ \ ,\ 2\mathbb{Z} \subset \mathbb{Z}\ )$

$\wedge$

$(\ |\mathbb{N}| = \infty, |\mathbb{Z}| = \infty, |2\mathbb{Z}| = \infty, |\mathbb{Q}| = \infty, |\mathbb{R}| = \infty, |\mathbb{C}| = \infty\ )$

مثال : دالاندي سیتونه معین (متناهی) دی

$X = \{\, x \mid$ x یو بحری اعظم $\}$
$Y = \{\, y \in \mathbb{Z} \mid -2 \le y \le 2\}$

X او Y هریو 5 عنصره لری . یعنې $|X| = |Y| = 5$
مګر $X \nsubseteq Y$ او $Y \nsubseteq X$

$W_1 : \ = \{w \in \mathbb{Z} \,|{-15} \le w \le 16 \quad \}$
$W_2 \coloneqq \{w \in \mathbb{Z} \,|(1 \le w \le 16\ ) \wedge (\text{w even (جفت)})\}$
$= \{2,4,6,8,10,12,14,16\}$

لیدل کیږی چې $W_2 \subseteq W_1$ او $|W_2| = 8$
دا لاندي سیتونه خالی دي

$W_3 := \{n \in \mathbb{N} \mid n < 0 \ \}$, $W4 := \{x \in \mathbb{Z} \mid x^2 = 3\}$

او $|W_3| = |W_4| = |W_5| = 0$

تعریف 0.3 : که چیری $X_1, X_2, \dots, X_n$ سیتونه وی، بیا :
اتحاد (Union):

$X_1 \cup X_2 \cup \dots \cup X_n \coloneqq \{x \mid \exists i \in \{1,2,3,..,n\}; x \in X_i\}$

تقاطع $(\boldsymbol{intersection})$:

$X_1 \cap X_2 \cap \dots \cap X_n \coloneqq \{x \mid x \in X_i, \forall i \in \{1,2,\dots,n\}\}$

په پورتنی مثال کی $W_1 \cup W_2 = W_1$ او $W_1 \cap W_2 = W_2$ دی

مثال: که $\mathbb{R}_+$ سیت دهغه حقیقی عددونه وي چې دصفرڅخه زیات اویا مساوی دی او $\mathbb{R}_-$ سیت دهغه حقیقی عددونه وي چې دصفرڅخه کم اویا مساوی دی . یعني

$\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \ \ge 0 \ \}$

$\mathbb{R}_- = \{x \in \mathbb{R} \mid x \ \le 0 \ \}$

دهغوی اتحاد د حقیقی اعدادو سیت او دهغوی تقاطع صفر ده.
یعني $\mathbb{R}_+ \cup \mathbb{R}_- = \mathbb{R}$ او $\mathbb{R}_+ \cap \mathbb{R}_- = \{0\}$

مثال:

$X \coloneqq \{x \in \mathbb{Z} \mid (-8 \le x \le 8)\}$
$Y \coloneqq \{x \in \mathbb{Z} \mid (-8 < x < 8)\}$
$8 \in X \implies 8 \in X \cup Y$
$-8 \in X \wedge -8 \notin Y \implies -8 \notin X \cap Y$
$5 \in X \wedge 5 \in Y \implies 5 \in X \cap Y$

مثال :

$A = \{a,b,c,d\}$, $B = \{d,e,f\}$, $C = \{a,b\}$
$A \cup B = \{a,b,c,d,e,f\}$, $A \cap B = \{d\}$
$C \subseteq A$, $A \cup C = \{a,b,c,d\} = A$, $A \cap C = \{a,b\} = C$
$A \setminus B = \{ a \in A \mid a \notin B \} = \{a,b,c\}$

$A \setminus C = \{ a \in A \mid a \notin C \} = \{ c, d \}$, $C \setminus A = \emptyset$

ځرنګه چې $C \subseteq \mathbf{A}$ دی . سیت $A \setminus C$ ته complement د C په A کې او
د $A \setminus B$ سیت ته relative Complement د B نظر A ته ویل کیږي

مثال:

$$W_1 := \{x \in \mathbb{R} \mid x < 0 \lor x > 0\}$$

W_1 سیت له هغوحقیقی اعدادو چې له صفرڅخه لوی یا ($\lor$) له صفرڅخه کوچنی وی، تشکیل شوی ده . یعنې:

$$W_1 = \mathbb{R} \setminus \{0\} = \mathbb{R}^*$$

W_2 سیت له هغوحقیقی اعدادو چې له صفرڅخه لوی اود ($\land$) صفرڅخه کوچنی وی تشکیل شوی ده . ځرنګه چې هغه ډول حقیقی عدد نه پیداکیږی. پس W_2 خالی ده یعنې: $W_2 = \emptyset$

تمرین 0.1 : دلاندې سیتونو عناصر (elements) پیدا کړی:

(a)

$$X := \{x \in \mathbb{Z} \mid (-1 \le x \le 6)\}$$

(b)

$$Y := \{x \in \mathbb{Z} \mid (1 \le x \le 7)\}$$

(c)

$$A: \{n \in \mathbb{Z} \mid 0 \le n \le 4\}$$
$$M := \{x \in \mathbb{Z} \mid x = n^2 - 4 , n \in A\}$$

(d) $X \cup Y$ او $X \cap Y$ پیداکړیی. البته دلته X او Y پورتنې سیتونه دې

تعریف : X یوسیت دی. که مونږ د X ټول فرعی سیتونه په p(X) وښیو. یعنې:

$$p(X) := \{A \mid A \subseteq X\}$$

p(X) د X د power set په نوم یادیږی.

مثال: که $X = \{a,b\}$ وي . په دی صورت دهغه فرعی سیتونه $A_1 = \{a\}$ ، $A_2 = \{b\}$، $A_3 = \{a,b\}$ او $\emptyset$ دي. یعنې:

$$p(X) = \{\emptyset, A_1, A_2, A_3\} \quad \land \quad |p(X)| = 4$$

که چیری X خالی سیت وي. پدی صورت $p(X) = \{\emptyset\}$ او $|p(\emptyset)| = 1$

قضیه : X او Y سیتولپاره دالاندې افادې صدق کوی:

(a)

$$X \subseteq Y \iff p(X) \subseteq P(Y)$$

(b)

$$p(X\cap Y)=p(X)\cap P(Y)$$

(c)

$$p(X)\cup p(Y)\subseteq p(X\cup Y)$$

ثبوت(a):

" $\Rightarrow$ "

$$A\in \mathrm{p(X)}\Rightarrow A\subseteq X \ \Rightarrow A\subseteq Y \ \Rightarrow \ A\in \mathrm{p(Y)}$$
$$\Rightarrow \ p(X)\subseteq P(Y)$$

$$x\in X \ \Rightarrow \{x\}\subseteq X \ \Rightarrow \ \{x\}\in p(X)$$
$$\Rightarrow \ \{x\}\in p(Y)$$ [د فرضيي له مخي]
$$\Rightarrow \{x\}\subseteq Y \ \Rightarrow \ x\in Y \ \Rightarrow \ X\subseteq Y$$

ثبوت(b):

$$A\in p(X\cap Y)\Rightarrow A\subseteq X\cap Y\Rightarrow A\subseteq X \ \wedge \ A\subseteq \ Y$$
$$\Rightarrow \ A\in p(X) \ \wedge \ A\in p(Y)\Rightarrow A\in p(X)\cap P(Y)$$
$$A\in p(X)\cap P(Y)\Rightarrow A\subseteq X \ \wedge \ A\subseteq Y\Rightarrow A\subseteq X\cap Y$$
$$\Rightarrow \ A\in p(X\cap Y)$$

په نتيجه کي: $p(X\cap Y)=p(X)\cap P(Y)$

ثبوت(c):

$$A\in p(X)\cup p(Y)\Rightarrow \ A\subseteq X \ \vee \ A\subseteq Y$$
$$\Rightarrow \ A\subseteq (X\cup Y)\Rightarrow \ A\in p(X\cup Y)$$

مگردالاندي رابطه صدق نه کوی:

$$p(X\cup Y) \ \subseteq p(X)\cup p(Y)$$

مثال:

$$X\coloneqq\{1,2\}, Y=\{2,3\}$$
$$p(X)=\{\emptyset,\{1\},\{2\},\{1,2\},\}$$
$$p(Y)=\{\emptyset,\{2\},\{3\},\{2,3\}\}$$
$$p(X)\cup p(Y)=\{\emptyset,\{1\},\{2\},\{1,2\},\{3\},\{2,3\}\ \}$$
$$X\cup Y=\{1,2,3\ \}$$
$$p(X\cup Y)=\{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\}\{2,3\},\{1,2,3\}\ \}$$

ليدل کيږی چه $\{1,3\}\notin p(X)\cup p(Y)$

قضيه: که د يومعين سيت $\mathrm{A_n}$ دعناصرو (elements) شمير n $(n\geq 0)$ وي، بيا هغه د Power set دعناصرو شمير 2^n دی.

ثبوت:غواړودا قضيه د complete induction له لياری نظرn ته ثبوت کړو.

په complete induction ثبوت کی دا دري لاندي حالتونه موجود دي
ایندکشن شروع : باید د n = 0 لپاره صدق وکړی
ایندکشن فرضیه: مونږ فرض کوو چه دټولو سیتونو لپاره چې درجه یی $n \geq 1$ وی ، صدق کوی
ایندکشن ثبوت : باید ثبوت شی چې د n+1 لپاره هم صدق کوی

ایندکشن شروع:

$$n = 0 \implies A_n = \emptyset \implies p(A_n) = \{\emptyset\} \implies |p(A_n)| = 1 = 2^0$$

ولیدل شو چه لمړی حالت صدق کوی

ایندکشن فرضیه: قبلوچه د n لپاره صدق کوی. یعنی: $|p(A_n)| = 2^n$

ایندکشن ثبوت: مونږ A_n او A_{n+1} په لاندي شکل تعریفوو:

$$A_n := \{a_1, a_2, \ldots., a_n\}$$
$$A_{n+1} := \{a_1, a_2, \ldots., a_n, a_{n+1}\}$$
$$A_n \subseteq A_{n+1} \implies p(A_n) \subseteq p(A_{n+1})$$

ایندکشن دفرضی له مخی د $p(A_n)$ د عناصروشمیر 2^n دی. مونږدغه عناصرپه لاندي شکل ښیو:

$$p(A_n) = \{s(1), s(2), \ldots, s(2^n)\}, \quad |p(A_n)| = 2^n$$
$$p(A_{n+1}) = p(A_n) \cup \{a_{n+1}\} = \{ s(1), s(2), \ldots, s(2^n),$$
$$s(1) \cup \{a_{n+1}\}, s(2) \cup \{a_{n+1}\}, \ldots, s(2^n) \cup \{a_{n+1}\} \}$$

پورته لیدل کیږی چه اتحاد د $\{a_{n+1}\}$ سره 2^n واری تکراریږی، نوبیا لیکلی شو:

$$|p(A_{n+1})| = |p(A_n)| + 2^n = 2^n + 2^n = 2.2^n = 2^{n+1}$$

مثال:

$$A_n := \{a_1, a_2\}$$
$$A_{n+1} := \{a_1, a_2, a_3\}$$

پدی مثال کی $n = 2$

$$p(A_n) = \{\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\} \} \}$$
$$|p(A_n)| = 2^2 = 4$$
$$p(A_{n+1}) = p(A_n) \cup \{a_3\} = \{\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\},$$
$$\{\emptyset, a_3\}, \{a_1, a_3\}, \{a_2, a_3\}, \{a_1, a_2, a_3\} \}$$
$$|p(A_{n+1})| = |p(A_n)| + 4 = 2^2 + 2^2 = 2.2^2 = 2^{2+1} == 2^3 = 8$$

تمرین:

(a) که $X = \{a, b, c\}$ وي. $p(X)$ او $|p(X)|$ پیداکړی

(b) که $X := \{x \in \mathbb{Z} \mid 4 \leq x^2 \leq 16\}$ وي. د X عناصر او $|p(X)|$ پیداکړی

تعریف 0.4: یوه تابع (function or mapping) له یوه سیت A څخه پر سیت B باندی یوه دا ډول رابطه ده چي دهرعنصر $a \in A$ لپاره یوازی یو عنصر $b \in B$ موجود وی چي د a د تصویر اویا انځور(map) په نوم یادیږي یعني باید:

$$\forall a \in A, \exists! b \in B \ ; \ f(a) = b$$

اوهغه په لاندې شکل ښودل کیږي :

$$f : A \longrightarrow B$$
$$a \longmapsto f(a) = b$$

f (a) د mapping یا image (تصویر یا انځور) د a نظر f په نوم , A د Domain په نوم , B د Codomain په نوم او f(A) د A د Range اویا image په نوم یادیږي. هر Range یو فرعی سیت *(subset)* د Codomain دی. دالاندي تابع د identity function په نوم یادیږی :

$$id : B \longrightarrow B$$
$$a \longmapsto id(a) = a$$

مثال: $A := \{ a , b , c \}$, $B := \{d , e , g , h \}$

$$f : A \longrightarrow B$$
$$a \longmapsto f(a) = e$$
$$a \longmapsto f(a) = g$$
$$b \longmapsto f(b) = d$$

دا ډول تعریف د f درست نه دی. ځکه لمړی داچي a دوه تصویرونه لری . دویم داچي c هیڅ تصویر نه لری.

مثال 0. 1 : د f لپاره دالاندي تعریفونه درست نه دي

(a)

$$f : \mathbb{Z} \longrightarrow \mathbb{N}$$
$$a \longmapsto 2a$$

ځکه : $a = -1 \in \mathbb{Z} \implies f(a) = f(-1) = -2 \notin \mathbb{N}$

(b)

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$r \longmapsto \sqrt{r}$$

ځکه د مثال په ډول $f(-2) = \sqrt{-2} \notin \mathbb{R}$

مګردالاندي تعریف د f لپاره درست دی

$$f: \mathbb{R} \longrightarrow \mathbb{C}$$
$$r \longmapsto \sqrt{r}$$

مثال: B:= {0 , 1 } , A:= { a , b , c }

(a)

$f: A \rightarrow B$, f(a) = 0 , f(b) = 1 , f(c) = 1

په دې مثال کښی range او codomain سره مساوی دي. یعنې هغه B دی

(b)

$g: A \rightarrow B$, g(a) = 1 , g(b) = 1 , g(c) = 1

په دی مثال کښی domain مساوی A , codomain مساوی B او range مساوی {1} نظر g *ته* دی

نوټ: دوه تابع f او g هغه وخت مساوی دي که چیری دواړه عین domain (د مثال په ډول A) او د هر $a \in A$ لپاره باید $f(a) = g(a)$ صدق وکړی.

تعریف 0.5 : $f : A \longrightarrow B$ یوه تابع (Mapping) ده.

f injective: $a, b \in A$, $f(a) = f(b) \Longrightarrow a = b$

(یعنې که مونږ $a, b \in A$ ولروچې $f(a) = f(b)$ وي. باید a = b شي)

اویاداچې: $a, b \in A$, $a \neq b \Longrightarrow f(a) \neq f(b)$

f surjective : ∀ b ∈ B ∃ a ∈ A ; f(a) = b

(یعنې دهر b ∈ B لپاره باید یو a ∈ A موجود وي چې f(a) = b شي)

f bijective : f injective ∧ f surjective

مثال: B:= {d , e , g } , A:= { a , b , c }

$$f: A \longrightarrow B$$
$$a \longmapsto f(a) = e$$
$$b \longmapsto f(b) = e$$
$$c \longmapsto f(c) = d$$

f یو injective نه دی. ځکه f(a) = f(b) = e مګر $a \neq b$ دی

f یو surjective هم نه دی .ځکه د g ∈ B لپاره هیڅ یو عنصرپه A کې نشته چې انځوریې g وی. یعنې:

$$\nexists x \in A ; \; f(x) = g$$

مثال: B:= {d , e } , A:= { a , b , c }

$$\begin{aligned} f&: A \longrightarrow B \\ a &\longmapsto f(a) = d \\ b &\longmapsto f(b) = d \\ c &\longmapsto f(c) = e \end{aligned}$$

f يو surjective دی مګر injective نه دی. ځکه f(a) = f(b) = d
مګر a ≠ b

مثال: A:= { a , b ,c } , B:= {d , e , g , h } . مونږ نشوکولای یوه تابع
$f: A \rightarrow$ B پیدا کړو چې surjective وی . ځکه
$|A| = 3 < 4 = |B|$ مګرد injective امکان شته.

مثال 0.2:

$$\begin{aligned} f&: \mathbb{Z} \longrightarrow \mathbb{Z} \\ a &\longmapsto 2a \end{aligned}$$

f يو injective دی . که مونږ $a , b \in \mathbb{Z}$ ولرو چې f(a) = f(b) وي.
باید ثبوت شی چې a = b کیږي

$$f(a) = f(b) \implies 2a = 2b \implies a = b$$

f يو surjective نه دی. ځکه په $\mathbb{Z}$ کي هیچ یوداسی عنصر نه پیداکیږی چې
تصویریي نظر f ته طاق اعداد (د مثال په ډول یو) وی .
یعنې $\nexists\, x \in \mathbb{Z}\ ;\ f(x) = 1$

مثال 0.3 :

(a) دالاندي تابع bijective ده

$$\begin{aligned} f&: \mathbb{R} \longrightarrow \mathbb{R} \\ a &\longmapsto 2a \end{aligned}$$

injective توب یی واضح دی او surjective هم ده.ځکه :

$$b \in \mathbb{R},\ a := \frac{b}{2} \in \mathbb{R} \implies f(a) = f\left(\frac{b}{2}\right) = 2.\frac{b}{2} = b$$

(b) دالاندي تابع Injective ده. مګر surjective نه ده

$$\begin{aligned} f&: \mathbb{N} \longrightarrow \mathbb{N} \\ n &\longmapsto f(n) = n + 1 \end{aligned}$$

$m,n \in \mathbb{N}\ ,\ f(m) = f(n) \implies m + 1 = n + 1 \implies m = n \implies f$ injective

دمثال په ډول د 1 لپاره هیڅ یوعدد m په $\mathbb{N}$ کښی نه پیداکیږی چې 1 = f(m) شی. پس surjective نه دی

مثال: دالاندي تابع نه injective او نه surjective ده

$$f: \mathbb{C} \longrightarrow \mathbb{R}$$
$$z = a + ib \longmapsto |z| = \sqrt{a^2 + b^2}$$

$z_1 = 3 + 4i \quad , z_2 = -3 - 4i$

$f(z_1) = |z_1| = \sqrt{3^2 + 4^2} = \sqrt{25} = 5$

$f(z_2) = |z_2| = \sqrt{(-3)^2 + (-4)^2} = \sqrt{25} = 5$

مگر $z_1 \neq z_2$ دی. پس injective نه ده.

Surjective هم نه ده. ځکه د هر $z \in \mathbb{C}$ لپاره $f(z) \geq 0$ دی

تمرین 0.2: معلوم کړی چې ولی دالاندي تابع نه injective او نه surjective کیدای شی

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$x \longmapsto x^2$$

تعریف 0.6 : که مونږ دوه تابع $f: A \longrightarrow B$ او $g: B \longrightarrow C$ ولرو.
$g \circ f : A \longrightarrow C$ د f او g د تابعو د ترکیب (mapping combination) په نوم یادیږی. په صورت عموم ترکیب د دوتابعوپه "∘" سره ښودل کیږی

مثال : پدی مثال کښی غواړو $g \circ f$ پیداکړو

$$g: \mathbb{Z} \longrightarrow \mathbb{R} \qquad\qquad f: \mathbb{N} \longrightarrow \mathbb{Z}$$
$$b \longmapsto b^2 - 1 \qquad\qquad a \longmapsto a + 1$$

$f(a) = a + 1 \in \mathbb{Z}$

$$g \circ f\,(a) = g(a+1) = (a+1)^2 - 1 = a^2 + 2a + 1 - 1$$
$$= a^2 + 2a$$

تمرین: $g \circ f$ پیدا کړی

(a)

$$g: \mathbb{N} \longrightarrow \mathbb{R} \qquad\qquad f: \mathbb{N} \longrightarrow \mathbb{N}$$
$$b \longmapsto 2\sqrt{b} \qquad\qquad a \longmapsto a + 1$$

(b)

$$g: \mathbb{N} \longrightarrow \mathbb{Q} \qquad\qquad f: \mathbb{N} \longrightarrow \mathbb{N}$$
$$b \longmapsto 2\sqrt{b} \qquad\qquad a \longmapsto a + 1$$

لیما 0.1 : که مونږ دوه تابع $f: X \to Y$ او $g: Y \to Z$ ولرو. بیا :

(a) $f\ injective \ \wedge\ g\ injective \ \Longrightarrow\ g \circ f\ injective$

(b) $f\ surjective\ \wedge\ \ g\ surjective\ \ \Longrightarrow g\circ f\ \ surjective$

(c) $g\circ f\ \ injective\ \ \Longrightarrow f\ injective$

(d) $g\circ f\ \ surjective \Longrightarrow g\ surjective$

(a) ثبوت: که چیری د $a,b\in X$ لپاره $g\circ f(a)=g\circ f(b)$ وی . پس باید ثبوت شی چې a = b کیږي

$g\circ f(a)=g\circ f(b)\Longrightarrow f(a)=f(b)$ [ځکه g یو $injective$]

$\Longrightarrow a=b$ [ځک f یو $injective$]

(b) ثبوت : باید ثبوت شی چې :

$\forall z\in Z,\exists x\in X; g\circ f(x)=z$

$f\ surj\ \Longrightarrow\ \forall y\in Y\ \exists\ x\in X; f(x)=y$

$g\ surj\ \Longrightarrow\ \forall z\in Z\ \ \exists\ y\in Y\ ; g(y)=z$

په نتیجه کې :

$g\big(f(x)\big)=g(y)=z\ \Longrightarrow g\circ f\ surj$

تمرین 0.3 : (c) و (d) دپورتنی لیما ثبوت کړی .

تمرین 0.4:

$f:\mathbb{Z}\ \longrightarrow\ \mathbb{Z}$, $g:\mathbb{Z}\ \longrightarrow\ \mathbb{Z}$, $h:\mathbb{Z}\ \longrightarrow\ \mathbb{Z}$

$n\longmapsto 2n$ $\quad n\longmapsto 3n+5$ $\quad n\longmapsto -6n$

(a) دلاندي توابعو ترکیب پیداکړی

$f\circ g\ ,\ g\circ f\ ,\ f\circ h\ ,h\circ f\ \ ,g\circ h\ ,h\circ g$

(b) کومی دهغوترکیبوڅخه injective اوکومی surjective دی

تعریف 0.7 : $f: A\rightarrow B$ یو bijective تابع ده . دهغی معکوسه تابع (inverse function) په لاندي ډول تعریف شوی دی :

$$f^{-1}: B\longrightarrow A$$
$$b\longmapsto a:=f^{-1}(b)$$

یعني د $b\in B$ تصویر نظر f^{-1} ته همغه عنصر $a\in A$ دی چې f(a) = b کیږي او f^{-1} هم *bijective* دی

$f\circ f^{-1}=\mathrm{id}: B\longrightarrow B\ \ \ \wedge\ \ f^{-1}\ \circ f\ =\mathrm{id}:\ A\rightarrow A$

مثال : دالاندي تابع Bijective ده

$$f:\mathbb{R}\longrightarrow\mathbb{R}$$
$$x\longmapsto 3x+2$$

د هغی معکوسه تابع (f^{-1}) لاندي شکل لري

$$f^{-1}:\mathbb{R}\longrightarrow\mathbb{R}$$
$$y\longmapsto\frac{y-2}{3}$$

ځکه:

$$f^{-1}(y)=\frac{y-2}{3}\Longrightarrow f\circ f^{-1}(y)=f\left(\frac{y-2}{3}\right)=\frac{3(y-2)}{3}+2=y$$

تمرين 0.5:

(a) ثبوت کړی چې د f تابع په پورتنی مثال کښی bijective ده .

(b) دلاندي تابع معکوس پیداکړی

$$f:\mathbb{R}\longrightarrow\mathbb{R}$$
$$x\longmapsto 2x+1$$

تعريف 0.8:

(a) معين (متناهی) سيت په لاندي ډول هم تعريف شوی دی:

يو M سيت ته هغه وخت معين ويل کيږی چې لاندي رابطی صدق وکړی:

$$f:M\longrightarrow M \quad \text{injective} \quad \Leftrightarrow \quad f:M\longrightarrow M \quad \text{surjective}$$

اويا په لاندي ډول :

$$\exists\ n\in\mathbb{N}\ \wedge\ \exists \text{ bijective } f:M\longrightarrow\{1,2,\dots,n-1\}$$
$$\Longrightarrow M \text{ finite (معين)}$$

(b) countable set (دشميروړ سيت):

يو سيت X د countable set (دشميروړسيت) په نوم ياديږی ، په دی شرط چې د X او د $\mathbb{N}$ (طبعی اعداد) ديو فرعی سيت (subset) ترمينځ يوه bijective تابع موجوده وي. که دا شرط موجود نه وي د uncountable set په نوم ياديږي.

يو سيت X د infinite countable (دشمير وړغيرمعين سيت) په نوم ياديږی، په دي شرط چې د X او$\mathbb{N}$ (طبعی اعداد) ترمينځ يوه bijective تابع موجوده وي. دمثال په ډول $\mathbb{Z}$ (تام اعداد) او $\mathbb{Q}$ (ناطق اعداد) infinite countable سيتونه دي. مگر $\mathbb{R}$ (حقيقی اعداد) يو uncountable سيت دی. اوس غواړو په يوه مثال کی وښيو چې $\mathbb{Z}$ يو دشميروړغيرمعين سيت دی.

$$f:\mathbb{Z}\longrightarrow\mathbb{N}$$

$$k\longmapsto f(k)=\begin{cases}2k & (k\geq 0)\\ 2(-k)-1 & (k<0)\end{cases}$$

:f injective

$m,n\in \mathbb{Z}\ ,\ f(m) = f(n)$

د m او n لپاره درى لاندي حالتونه موجود دي:

$1.\quad m,n \geq 0 \Rightarrow f(m) = 2m \wedge f(n) = 2n \Rightarrow m = n$
$\Rightarrow$ f injective

$2.\quad m \geq 0 \wedge n < 0 \Rightarrow f(m) = 2m \wedge f(n)= 2(-n)-1$

څرنګه چې n < 0 انتخاب شويدى ، بايد 2(-n)> 0 او 2(-n)-1 يو طاق عدد وي. په تيجه کى د f(m) = 2m = 2(-n)-1 = f(n) حالت امکان نه لري.

$3.\quad m,n < 0 \Rightarrow f(m)= 2(-m)-1 \wedge f(n)= 2(-n)-1$

$f(m)= 2(-m)-1 = f(n)= 2(-n)-1 \Rightarrow m = n$

$\Rightarrow$ f injective

f surjective: د $x\in \mathbb{N}$ لپاره دوه لاندي حالاتونه امکان لري :

لمړى حالت: x يو جفت عدد دى

x even $, x \geq 0 \Rightarrow \exists\, k\in \mathbb{Z}\, ;\, 2k = x \Rightarrow k = \frac{x}{2}$

$\Rightarrow f(k) = f(\frac{x}{2}) = 2.\frac{x}{2} = x \Rightarrow$ f surjective

دويم حالت : x يوطاق عدد دى

$x = 2.(-k) - 1 \Rightarrow k = -\frac{x+1}{2} \in \mathbb{Z}$

$f(k) = f(-\frac{x+1}{2}) = 2.(- (-\frac{x+1}{2}) - 1 = x + 1 - 1 = x$

$\Rightarrow$ f surjective

په نتيجه کي f بايجکتيف دى او $\mathbb{Z}$ نظر تعريف ته يو دشميرور غيرمعين سيت دى.

قضيه 0.1 : که A يو معين (متناهي) سيت وى . بيا ديوى تابع $f: A \to A$ لپاره دالاندي افادي ديوبل سره معادلي دي .

(i) f يو injective دى
(ii) f يو surjective دى
(iii) f يو *bijective* دى

ثبوت : څرنګه چې A معين دى اومونږ فرض کوو چې n مختلف عنصره لرى . يعني

$$A = \{ a_1, a_2, \dots, a_n \}$$

(ii) ⇐ (i)

که f یو *surjective* نه وی . داپه دی معنی چې:

$$f\ not\ surjective \implies f(A) \neq A \implies \exists a \in A ; a \notin f(A)$$

یعنې د f(A) د عناصروشمیر له n څخه کم دی . که $|f(A)|$ = m وی د Birichlet پرنسیپ وای. که چیری n اوبجکت په m (m<n) روکو کښنی تقسیم شی. په یوه روک کښنی باید دوه object وی . داپدی معنی چې f یو injective نه دی . مگر دا د فرضیی تضاد دی. پس باید f یو surjective وی.

(i) ⇐ (ii)

که f یو *injective* نه وی . دا په دی معنی چې:

$$f\ not\ injective \implies \exists a, b \in A ; a \neq b \ \wedge \ f(a) = f(b)$$

پدی حالت کې f(A) کولای شی اعظمی n-1 عنصر ولری . یعنې باید f(A) $\neq A$ وی . مگردا خلاف د فرضی ده. ځکه f یو surjective فرض شوی وه. پس باید f injective وی .

نوټ:

(a) د دومعینوسیتو A او B لپاره هم 0.1 قضیه صدق کوی. پدی شرط چې

$|A| = |B|$ وي.

(b) دالاندي مثالونه ښي چې 0.1 قضیه دغیرمعین سیت لپاره صدق نه کوې

مثال 0.4:

(a)

$$f : \mathbb{N} \to \mathbb{N}$$

$$n \longmapsto f(n) = \begin{cases} n & (\text{که } n \text{ طاق}) \\ \frac{n}{2} & (\text{که } n \text{ جفت}) \end{cases}$$

f یو injective نه دی. ځکه:

$$f(3) = 3 = \frac{6}{2} = f(6) \implies f\ not\ injective$$

f مگر surjective دی : k∈ ℕ

لمړی حالت: که چیری k طاق وی. پدی صورت کی $f(k) = k$ کیږی او f یو surjective دی

دویم حالت: که چیری k جفت وي. په دی صورت:

$$\exists\, n \in \mathbb{N} \;;\; k = \frac{n}{2} \implies n = 2k \implies f(n) = f(2k) = \frac{2k}{2} = k$$
$$\implies f \text{ surjective}$$

(c) که چیری B یو معین سیت او A د هغه proper subset (یعنې $A \subset B$) وی. په دی صورت مونږنشوکولای یوه bijective تابع ددی دواړو سیتونو ترمینځ پیده کړو. مګردغیرمعینو سیتونو ترمینځ بیا دا امکان شته. چې لاندي مثالونه دا واضح کوی

مثال 0.5:

(i)

$$f : \mathbb{N}_0 \to \mathbb{Z}$$
$$x \longmapsto f(x) = \begin{cases} \frac{x}{2} & (\text{که } x \text{ جفت}) \\ \frac{-(x+1)}{2} & (\text{که } x \text{ تاق}) \end{cases}$$

البته دلته 0 جفت عدد فرض شویدی

د *injective* د ثبوت لپاره دالاندي دری حالته په پام کی نیسو:

$x, y \in \mathbb{N}$

case 1: $f(x) = \frac{x}{2}$, $f(y) = \frac{y}{2}$

$$f(x) = f(y) \implies \frac{x}{2} = \frac{y}{2} \implies 2.x = 2.y \implies x = y$$

case 2: $f(x) = \frac{-(x+1)}{2}$, $f(y) = \frac{-(y+1)}{2}$

$$f(x) = f(y) \implies \frac{-(x+1)}{2} = \frac{-(y+1)}{2} \implies -2.x - 2 = -2.y - 2$$
$$\implies x = y$$

case 3 : $f(x) = \frac{x}{2}$, $f(y) = \frac{-(y+1)}{2}$

$$f(x) = f(y) \implies \frac{x}{2} = \frac{-(y+1)}{2} \implies 2.x = -2.y - 2 \implies x + y = 1$$

$x + y = 1$ امکان نه لری ، ځکه x او y طبعی اعداد دی.

ولیدل شول چې دریم حالت امکان نه لری. مګر په لمړی او دویم حالت کښی f اینجکتیف دی. f یو surjective هم دی. ځکه:

د $y \in \mathbb{Z}$ لپاره درې لاندي حالته موجود دي:

case 1 : y = 0

$\frac{x}{2} = y = 0 \quad \vee \quad \frac{-(x+1)}{2} = y = 0$

$\Longrightarrow x = 0 \ \vee \ -(x+1) = 0$

څرنګه چې $0 \notin \mathbb{N}$ دی. پس باید $-(x+1) = 0$ وی.

$-(x+1) = 0 \quad \Longrightarrow \quad x = -1$

$f(-1) = \frac{-(-1+1)}{2} = 0$

case 2 : y > 0

$x := 2y \in \mathbb{N} \quad \Longrightarrow f(x) = f(2y)$

$= \frac{2y}{2} = y$ [ځکه 2y جفت دی]

case 3 : y < 0

$x := -2y-1 \in \mathbb{N} \quad \Longrightarrow f(x) = f(-2y-1)$

$= \frac{-(-2y-1+1)}{2}$ [ځکه -2y-1 طاق]

$= \frac{2y}{2} = y$

په هردرې حالتوکښې ولیدل شوه چې دهر $y \in \mathbb{Z}$ لپاره یو x په $\mathbb{N}$ کښې پیداکیږی چې $f(x) = y$ شي. $\mathbb{Z}$ او $\mathbb{N}$ دواړه غیرمعین دی او $\mathbb{N} \subset \mathbb{Z}$ هم صدق کوی. بیاهم *bijective* ددواړوسیټونوترمینځ موجود دی

(ii) دا لاندي Exponentialfunction بایجکټیف ده:

$\exp : \mathbb{R} \longrightarrow \mathbb{R}_+$

$x \longmapsto e^x$

e د اویلرعدد (Eulers Number) په نوم یاددیږی

$e = 2.718281828459$

: injective

$x, y \in \mathbb{R}$, $\exp(x) = \exp(y)$

$\Longrightarrow e^x = e^y \Longrightarrow x = y \Longrightarrow$ exp injective

:surjective

$y \in \mathbb{R}_+$

$x := \ln(y) \Longrightarrow y = e^x = \exp(x) \Longrightarrow$ exp surjective

$\mathbb{R}_+$ او $\mathbb{R}$ دواړه غیرمعین دي او $\mathbb{R}_+ \subset \mathbb{R}$ هم صدق کوی. بیاهم *bijective* ددواړوسیټونوترمینځ موجود دی.

تمرين 0.7 : معلوم کړی چې کومي دلاندي توابع څخه surjective , injective اويا bijective دي

(a)

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto x^2 + 1$$

(b)

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto 3x - 4$$

تعريف 0.9 : د A_i (i=1,2,3,…,n) سيټونو لپاره direct product of Sets په لاندي ډول تعريف شوی دی:

$$A_1 \times A_2 \times \ldots . \times A_n$$
$$:= \{(a_1, a_2, \ldots ., a_n) \,|\, a_i \in A_i \,, i = 1,2, \ldots, n\}$$

که مونږ $A = A_1 \times A_2 \times A_3 \times \ldots . \times A_n$ وضع کړو. پدی صورت هر عنصر $a \in A$ لاندي شکل لري:

$$a = (a_1, a_2, a_3, \ldots, a_n)$$

$(a_1, a_2, a_3, \ldots, a_n)$ ته n-tupel ويل کيږی اومساويتوب د دو n – tupel دا ډول تعريف شوی دی:

$$a = (a_1, a_2, a_3, \ldots, a_n) \,, b = (b_1, b_2, b_3, \ldots, b_n) \in A$$
$$a = b \;:\Leftrightarrow\; a_i = b_i \;\forall\, i \in \{1,2, \ldots, n\}$$

که $A = A_1 = A_2 = A_3 = \cdots = A_n$ وی په دی صورت direct product د A_i سيټونو د A^n په شکل ليکل کيږي.

direct product د Cartesian product په نوم هم يادېږي اوپه هندسه کښی تری زياده استفاده کيږي. که د A سيټ m عنصر اود B سيټ n عنصر ولری. يعني $|A| = m$ ، $|B| = n$ او که G سيټ direct product د A او B وی. يعني G = AxB . په دی صورت د G دعناصرو شمير m.n دی. يعني

$$|G| = |AxB| = |A|.|B| = m.n$$

پورته رابطه دزياتو معينو سيټونو لپاره A_i (i=1,2,…,n) هم صدق کوی .

مثال:

A = {1,2,3} , B = {a,b,c,d}

G = AxB = {1,2,3} x {a,b,c,d}

= { (1,a),(2,a),(3,a),{1,b),(2,b),(3,b),(1,c),(2,c),(3,c),(1,d)

,(2,d),(3,d) }

لیدل کیږی چې: $|G| = 3.4 = 12$

مثال 0.6:

$\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$

$f: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$(x_1, x_2) \mapsto (2x_1, x_2)$

f injective:

$x = (x_1,x_2)$, $y = (y_1,y_2) \in \mathbb{R}^2$

که چیرې $f(x) = f(y)$ وي. باید ثبوت شي چې $x = y$ دی

$f(x) = f(y) \implies (2x_1, x_2) = (2y_1, y_2)$

$\implies 2x_1 = 2y_1 \wedge x_2 = y_2 \implies x_1 = y_1 \wedge x_2 = y_2$

$\implies x = y$

$\implies$ f injective

f surjective:

$y = (y_1,y_2) \in \mathbb{R}^2$

باید یو $x = (x_1,x_2) \in \mathbb{R}^2$ موجود وي چې $f(x) = y$ شی

$f(x) = f(x_1, x_2) = (2x_1, x_2) := y = (y_1,y_2)$

$\implies 2x_1 = y_1 \wedge x_2 = y_2 \implies x_1 := \frac{y_1}{2} \wedge x_2 := y_2$

$\implies f(x) = f(x_1, x_2) = f(\frac{y_1}{2}, y_2) = (2.\frac{y_1}{2}, y_2) = (y_1, y_2) = y$

$\implies$ f surjective

په نتیجه کې f یو bijective دی.

تمرین 0.7 : دلاندي سیتونو عناصر (elements) پیدا کړی :

$W := \{(x,y) \in \mathbb{Z}x\mathbb{Z} \,|\, (x + y = 0) \wedge (-3 \le x, y \le 3)\}$

$X := \{(x,y) \in \mathbb{Z}x\mathbb{Z} | (x^2 = y^2) \wedge (-3 \le x, y \le 3)\}$

$Y := \{(x,y) \in \mathbb{Z}x\mathbb{Z} | (x = 0 \vee y = 0) \wedge (-3 \le x, y \le 3)\}$

(b)

$W := \{(x_1, x_2, x_3) \in \mathbb{R}^3 | x_2 = x_3\}$

$u = (1,0,1)$, $v = (2,0,3)$, $w = (0,1,0)$

معلوم کړی چه کوم یود w,v,u په W کی شامل اوکوم شامل نه دي

(c)

$H := \{ (x_1,x_2,x_3,x_4) \in \mathbb{R}^4 \,|\, x_1+3x_2+2x_4=0 , 2x_1,x_2+x_3=0\}$

$u=(1,2,0,2)$, $v=(3,-1,-5,0)$, $w=(-1,1,1,-1)$

معلوم کړی چه کوم یود w,v,u په H کی شامل اوکوم شامل نه دي

تمرین 0.8 : کومی لاندي تابع injective , surjective او bijective دی

(a)

$$f : \mathbb{R}x\mathbb{R} \longrightarrow \mathbb{R}$$
$$(x_1, x_2) \longmapsto x_1 + x_2$$

(b)

$$f : \mathbb{R}x\mathbb{R} \longrightarrow \mathbb{R}$$
$$(x_1, x_2) \longmapsto {x_1}^2 + {x_2}^2 - 1$$

تعریف 0.10: یوه رابطه (relation) "~" پریوسیت $A \neq \phi$ باندی دلاندي خواصوسره د equivalence relation (معادله رابطه) په نوم یادیږی .

$a, b, c \in A$

(i) a~a (reflexive)

(ii) a~b ⇒ b~a (symmetric)

(iii) a~b ∧ b~c ⇒ a~c (transitive)

په ځینو کتابوکې reflexive ته انعکاس، symmetric ته متناظر او transitive ته انتقالي ویل شوي دی.

مثال: د مساوات رابطه "=" پریوه سیت $A \neq \phi$ باندی یوه معادله رابطه (eq-relation) ده.

reflexive: a = a ⇒ a ~ a ($\forall\ a \in A$)

symmetric: a~b ⇒ a = b ⇒ b = a

⇒ b~a ($\forall\ (a, b) \in AxA$)

transitive: a~b ∧ b~c ⇒ a = b ∧ b = c ⇒ a = c

⇒ a~c $\forall\ (a, b), (b, c) \in AxA$

مثال: پر $\mathbb{Z}$ باندی دالاندي رابطه په پام کې نیسو:

a ~ b :⇔ a ≤ b ($(a, b) \in \mathbb{Z}x\mathbb{Z}$)

پورتنی رابطه reflexive او transitive ده. مګر symmetric نه ده. ځکه:

$2 \leq 3 \Rightarrow 2 \sim 3$

$3 \nleq 2 \Rightarrow 3 \nsim 2$

پس پورتنی رابطه یوه معادله رابطه (eq-relation) نه ده .

مثال 0.7: پر $\mathbb{Z}$ باندی دالاندي رابطه یوه معادله رابطه (eq-relation) ده .
$(a,b) \in \mathbb{Z}x\mathbb{Z}$

$a \sim b :\Leftrightarrow 2 \mid a - b$ ($a - b$ پر 2 قابل د تقسیم دی)

:reflexive

$a - a = 0 \Rightarrow 2 \mid 0 \Rightarrow a \sim a$

: symmetric

$(a,b) \in \mathbb{Z}x\mathbb{Z}$, $a \sim b \Rightarrow 2|a - b \Rightarrow \exists\, q \in \mathbb{Z} ; a - b = 2q$

$\Rightarrow b - a = 2.(-q)$

$\Rightarrow 2|b - a \Rightarrow b \sim a \Rightarrow$ "$\sim$" symmetric

: transitive

$(a,b),(b,c) \in \mathbb{Z}x\mathbb{Z}$, $a \sim b \wedge b \sim c \Rightarrow 2|a - b \wedge 2|b - c$

$\Rightarrow \exists\, m \in \mathbb{Z} ; a - b = 2m \wedge \exists\, n \in \mathbb{Z} ; b - c = 2n$

$\Rightarrow b = a - 2m \wedge c = b - 2n$

$\Rightarrow c = a - 2m - 2n = a - 2(m+n)$

$\Rightarrow c - a = -2(m+n) \Rightarrow a - c = 2(m+n) \Rightarrow 2|a - c$

$\Rightarrow$ "$\sim$" transitive

ثبوت شو چې "$\sim$" یوه معادله رابطه (eq-relation) ده .

مثال: پر $\mathbb{Z}$ (تام اعداد) دا "$\sim$" رابطه (relation) په لاندي ډول تعریف شوی ده : $a,b,c \in \mathbb{Z}$

$a \sim b :\Leftrightarrow a.b \neq 0$

$a \sim b \Rightarrow a.b \neq 0 \Rightarrow b.a \neq 0 \Rightarrow b \sim a \Rightarrow$ "$\sim$" symmetric

$a \sim b \wedge b \sim c \Rightarrow a.b \neq 0 \wedge b.c \neq 0$

$\Rightarrow a \neq 0 , b \neq 0 , c \neq 0$

$\Rightarrow a.c \neq 0 \Rightarrow a \sim c \Rightarrow$ "$\sim$" transitive

مګر reflexive نه ده . ځکه که $0 \sim 0$ وی ، باید $0.0 \neq 0$ شي.

پس "$\sim$" یوه معادله رابطه (eq-relation) نه ده.

تمرین0.9:

(a) X د یوه ښونځی شاګردان دی . پر X بانه دي لاندي رابطه (relation) تعریف شوی ده. $a,b \in X$

a~b: ⇔   a د b سره په یوه ټولګی کی دی

ثبوت کړی چې "~" یوه معادله رابطه (eq-relation) ده

(b) X د ساینس دپوهنځي محصلین دی. پر X بانه دي لاندي رابطه (relation) تعریف شوی ده. a,b ∈ X

a~b: ⇔   a د b سره هم سنه دی

ثبوت کړی چې "~" یوه معادله رابطه (eq-relation) ده

تمرین 0.10 : پر $\mathbb{Q}$ (ناطق عددونه) باندی دا لاندي رابطه تعریف شویده:

$a, b \in \mathbb{Q}$

a~b: ⇔ $a - b \in \mathbb{Z}$

(a) ثبوت کړی چه "~" یوه معادل رابطه (eq-relation) ده

(b) کومي لاندینی روبطی درستي دي

$\frac{26}{12} \sim \frac{14}{12}$, $\frac{9}{3} \sim \frac{10}{5}$, $\frac{2}{3} \sim \frac{1}{6}$, $\frac{8}{7} \sim \frac{1}{7}$, $\frac{6}{7} \sim \frac{1}{8}$

تعریف 0.11: پر $X \neq \phi$ سیت بانه دي یوه „ ~ „ equivalence relation (معادله رابطه) تعریف شوی ده

$[x]_\sim := \{ y \in X \mid x \sim y \}$

$[x]_\sim$ ته equivalence class (معادل کلاس) ویل کیږي. که مونږ معادله رابطه (eq-relation) د 0.6 مثال په پام کې ونیسو. د مثال په ډول

$[5]_\sim = \{ y \in X \mid 5 \sim y \} = \{ y \in X \mid 2|5 - y \}$

$= \{ \ldots, -5,-3,-1,1,3,5, 7, 9, 11, \ldots \}$

قضیه 0.2 : $X \neq \phi$ سیت او „ ~ „ یوه معادله رابطه (eq-relation) پر X ده. بیا دالاندي افادي صدق کوي :

(a) $X = \bigcup_{x \in X} [x]_\sim$

(b) $[x]_\sim \neq \phi \quad \forall x \in X$

(c) $[x]_\sim \cap [y]_\sim \neq \emptyset \iff x \sim y \iff [x]_\sim = [y]_\sim$

(a) ثبوت : $\bigcup_{x \in X} [x]_\sim \subseteq X$ واضح دی

$x \in X \implies x \in [x]_\sim \quad [\sim \text{ reflexive}]$

$\implies [x]_\sim \neq \phi \ \wedge \ X \subseteq \bigcup_{x \in X} [x]_\sim$

په عین وخت کې (b) هم ثبوت شو.

(c) ثبوت :

$u \in [x]_{\sim} \cap [y]_{\sim}$

$\Rightarrow x \sim u \quad \wedge \quad y \sim u$

$\Rightarrow x \sim u \quad \wedge \quad u \sim y \quad [\sim \text{ symetric }]$

$\Rightarrow x \sim y \quad [\sim \text{ transitive }]$

$x \sim y \quad \Rightarrow \quad \forall \; u \in [x]_{\sim} \; ; \; x \sim u$

$\wedge \; x \sim y \quad [\sim \text{ symetric } \wedge \text{ transitive }]$

$\Rightarrow y \sim u \quad [\sim \text{ symetric } \wedge \text{ transitive }] \Rightarrow u \in [y]_{\sim}$

$\Rightarrow [x]_{\sim} \subseteq [y]_{\sim}$

همدا ډول کولاې شو ثبوت کړو چې $[y]_{\sim} \subseteq [x]_{\sim}$

له بلي خوا که :

$[x]_{\sim} = [y]_{\sim} \Rightarrow x \sim y \Rightarrow [x]_{\sim} \cap [y]_{\sim} \neq \emptyset$

تعریف 1.12: $n, k \in \mathbb{N}$

$n! = 1.2.3.....n$

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!.(n-k)!} & 0 \le k \le n \\ 0 & k > n \end{cases}$$

$n!$ د factorial او $\binom{n}{k}$ د binomial coefficient په نوم یادیږي. البته دلته که k او n مساوی اویا k مساوی صفروي ، پدی صورت $\binom{n}{k}$ په لاندي ډول تعریف شویده:

$\binom{n}{0} = \binom{n}{n} = 1$

مثال:

$5! = 1.2.3.4.5 = 120$

$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{120}{6.2} = \frac{120}{12} = 10$

تعریف 0.13 : (mathematical logic and De Morgan`s Laws)

مونږ دلته غواړو په مختصرډول د ریاضیاتو منطق (mathematical logic) او De Morgan قانون د مثالو سره تشریح کړو.

(a) Boolean Operators : دالاندي عمليات (operatotrs) د Boolean Operators په نوم یادیږي:

∧ : logical **and** (conjuction) (او)
∨ : logical **or** (disjuction (یا)

د مثال په ډول مونږ دا لاندي افادي (statments) لرو:

P : د کابل د پوهنتون محصل توب
Q : په پښتوژبه خبروکولو توان
R : د هرات اوسیدونکی

مثال: احمد د بلخ اوسیدونکی ، کابل د پوهنتون محصل اوپه پښتوخبري کولای شی دلته د P اوQ افادی صدق کوی. مګرد R افاده صدق نه کوی. که مونږ هغه افادی چې صدق کوي په T (true) اوکه صدق نه کوي په F (false) سره وښیو، بیا کولای شو چې هغه په جدول کی لاندي شکل لري:

∧ (**and**) :

P	Q	R	P ∧ Q	P ∧ R	Q∧ R
T	T	F	T	F	F

∨ (or) :

P	Q	R	P ∨ Q	P ∨ R	Q ∨ R
T	T	F	T	T	T

مثال: مونږ دالاندي افادي لرو:

P : کباب خوړل
Q : کولا ښبنل
R : شربت ښبنل
P∧ Q : محمود غواړي کباب وخوری او کولا وښبنی
Q∨R : محمود غواړي کولا اویا شربت وښبنی
P∧(Q∨R) : محمود غواړي کباب وخوری او (کولا یا شربت وښبنی)
Q ∨(P∧R) **:** محمود غواړي کولا وښبنی او یا (کباب وخوری او شربت وښبنی)

نوت : P ، Q و R دري افادیه (statments) دي. په عمومی ډول د Boolean Operators دا لاندي خواص لري :

تبدیلی (commutative):
$P \wedge Q = Q \wedge P$

اتحادی (associativ**e**):

$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$
$P \vee (Q \vee R) = (P \vee Q) \vee R$

توزیعی (distributive):

$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$
$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

(b) د مرجن قانون (De Morgen`s Laws) :
مونږ هغه دری افادی p ، Q او R د پورتنی مثال په پام کی نیسو

logic not: ¬

¬P : کباب نه خوړل

¬ R: شربت نه ښښل

¬Q : کولا نه ښښل

¬(P ∧ Q) (Negation of a conjunction)

¬(P∨Q) (Negation of a disjunction)

(b) دمیرجن قانون (De Morgen`s Laws) :

$\neg(P \wedge Q) = \neg P \vee \neg Q$ [محمود نه غواړی کباب وخوری یا کولا وښښی]

$\neg(P \vee Q) = \neg P \wedge \neg Q$
[محمود نه غواړی کباب وخوری او نه غواړی کولاوښښی]

مثال:

(a) د p او Q افادي په لاندي ډول تعريف شوي دي:

P: $x \le 100$, Q: $x > 40$

پدی صورت:

$P \wedge Q = \{ x \le 100 \wedge x > 40 \}$
$\neg(P \wedge Q) = (\neg P) \vee (\neg Q) = (x > 100) \vee (x \le 40)$

(b) p ، Q اوR په لاندي ډول تعريف شوي دي:

P: $x = 10$, Q: $x = -10$, R: $x^2 = 100$

لاندي رابطی لیکلی شو:

$P \Rightarrow R$, $Q \Rightarrow R$
$R \nRightarrow P$, $R \nRightarrow Q$

$R \Leftrightarrow P \vee Q$

De Mo rgen`s Laws for Sets :

$A,B \subseteq X$

$A^c := X \setminus A = \{ a \in X \mid a \notin A \}$

A^c complement of A in X

$B^c := X \setminus B = \{ a \in X \mid a \notin B \}$

B^c complement of B in X

$(A \cup B)^c = A^c \cap B^c$

$(A \cap B)^c = A^c \cup B^c$

مثال :

$X := \{ a,b,c,d,e,f,g,h,8,9\}$, $A := \{ a,b,c,d\}$, $B := \{c,d,e,f,\}$

$A \cup B = \{a,b,c,d,e,f\}$, $A \cap B = \{c,d\}$

$A^c = \{e,f,g,h,8,9\}$, $B^c = \{a,b,g,h,8,9\}$

$(A \cup B)^c = \{g,h,8,9\} = A^c \cap B^c$

$(A \cap B)^c = \{a,b,e,f,g,h,8,9\} = A^c \cup B^c$

لمړی فصل

(Group)ګروپ

تعریف 1.1 : یوه دوه ګونی رابطه (Binary operation) "$\oplus$" پریوه ست $M \neq \phi$ په لاندي ډول تعریف شویده:

$$\oplus: M \times M \longrightarrow M$$
$$(a, b) \longmapsto a \oplus b$$

یعني د هر $(a, b) \in M \times M$ فقط یوازی یو عنصر $c \in M$ موجود دی چې $c = a \oplus b$ شی.

مثال : په لاندي مثال کښی یوه دوه ګونه رابطه (Binary operation) " $\oplus$ " پر $\mathbb{Z}$ (تام اعداد) تعریف شوی ده

$$\oplus : \mathbb{Z} \, x \, \mathbb{Z} \longrightarrow \mathbb{Z} \, .$$
$$(\mathrm{a}, \mathrm{b}) \longmapsto \mathrm{a} \oplus \mathrm{b} = 2\mathrm{a} - \mathrm{b}$$

دهر $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ لپاره فقط یوازی یو $c \in \mathbb{Z}$ موجود دی چې $c = a \oplus b$ شي. مګرکه $\oplus$ په لاندي ډول پر $\mathbb{N}$ (طبیعي اعداد) باندی تعریف کړو

$$\oplus: \mathbb{N} \, x \mathbb{N} \longrightarrow \mathbb{N}$$
$$(\mathrm{a}, \mathrm{b}) \longmapsto \mathrm{a} \oplus \mathrm{b} = 2\mathrm{a} - \mathrm{b}$$

دا دوه ګونی رابطه (Binary operation) نه ده . ځکه که $a = 2$ او $b = 6$ وی

$$a \oplus b = 2a - b = 2 \cdot 2 - 6 = -2 \notin \mathbb{N}$$

مثال : په لاندي مثال کښی یوه دوه ګونه رابطه (Binary operation) " $\odot$ " پر $\mathbb{R}$ (حقیقی اعداد) تعریف شوی ده

$$\odot : \mathbb{R} \, x \, \mathbb{R} \longrightarrow \mathbb{R}$$
$$(\mathrm{a}, \mathrm{b}) \longmapsto \mathrm{a} \odot \mathrm{b} = \frac{1}{2} (\mathrm{a} + \mathrm{b})$$

مګر که $\odot$ په لاندي ډول پر $\mathbb{Z}$ (تام اعداد) تعریف کړو

$$\odot: \mathbb{Z} \, x \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(\mathrm{a}, \mathrm{b}) \longmapsto \mathrm{a} \odot \mathrm{b} = \frac{1}{2} (\mathrm{a} + \mathrm{b})$$

دایوه دوه ګونه رابطه نه ده . ځکه که $a = 2$ او $b = 3$ وی

$a\odot b = \frac{1}{2}(a + b) = \frac{1}{2}(2 + 3) = \frac{5}{2} \notin \mathbb{Z}$

تعریف 1.2 : یو سیت $M \neq \phi$ له یوی دوه ګوني رابطی $\oplus$ سره د الجبری جوړښت (algebraic structure) په نوم یادیږی او مونږهغه په $(M, \oplus)$ سره ښیو. یو سیت M له دو دوه ګونورابطو (Binary operations) $\oplus$ او $\odot$ سره مونږ په $(M, \oplus, \odot)$ ښیو. د مثال په ډول $(\mathbb{Z}, +, .)$, $(\mathbb{R}, +, .)$ او $(\mathbb{C}, +, .)$ الجبري جوړښت (ساختمان) لری چې هریوی دوه دوه ګوني رابطی "+" او " . " لری

د یو $(M, \oplus)$ الجبری جوړښت (ساختمان) لپاره لاندي خواص تعریف شویدي:

(i) اتحادی(associativity)

$$a\oplus(b\oplus c) = (a\oplus b)\oplus c \qquad (\ \forall a, b, c \in M\ )$$

(ii) نظر $\oplus$ ته د چپ عینیت (left identity) خاوند دی، پدی شرط چې یو $e \in M$ موجود وی چې $e\oplus a = a$ اوډښی عینیت (right identity) خاوند دی پدی شرط چې $a\oplus e = a$ $(\forall a \in M)$ شی . که د چپ عینیت او ښی عینیت سره مساوی وي ، بیا د عینیت عنصر په نوم یادیږی.

(iii) یو$b \in M$ د یوه $a \in M$ د چپ معکوس (left inverse) په نوم یادیږی، په دی شرط چې $b\oplus a = e$ اوښی معکوس (right inverse) ورته واي، که $a\oplus b = e$ وی . البته e دلته عینیت عنصر دی.

(iv) تبدیلی(commutative)

$$a\oplus b = b \oplus a \qquad (\ \forall a, b \in M\ )$$

نوت: $(M, \oplus, \odot)$ یو الجبری ساختمان دی. لاندي خواص ته توزیعی (distributive) ویل کیږی

$$\forall a, b, c \in M\ , \quad a\odot(b\oplus c) = (a\odot b)\oplus(a\odot c)$$

$$\wedge$$

$$(b\oplus c)\odot a = (b\odot a)\oplus(c\odot b)$$

مثال:

(a) $M := \{-1, 1\} \subset \mathbb{R}$

$$\cdot : M \times M \longrightarrow M$$

$$(a, b) \longmapsto a \cdot b$$

د M سیت نظر ضرب " · " ته یو الجبری ساختمان لری. مګرنظر جمع "+" ته نه لری. ځکه $1 + 1 = 2 \notin M$. یعني $(M, \cdot)$ یو الجبری جوړښت

(ساختمان) دی. مګر (M,+) نه دی.

(b) د $M:=\{-1,1,i,-i\} \subset \mathbb{C}$ سیت نظر ضرب ".„ یو الجبری ساختمان لری. ځکه

$(-1).(-1) = 1 \in M$, $(-1).(1) = -1\in M$, $(-1).i = -i\in M$,

$(-1).(-i) = i\in M$, $1.1 = 1\in M$, $1.i = i \in M$, $1.(-i) = -i\in M$,

$i.i = -1\in M$, $i.(-i) = -1.(i^2) = (-1).(-1) = 1\in M$,

$(-i).(-i) = 1.(i^2) = 1.(-1) = -1\in M$

مګر M نظر جع "+„ ته الجبری ساختمان نه لری . ځکه:

$(-1)+(-1) = -2 \notin M$

(c) $(\mathbb{N}_0,+)$ هم الجبری ساختمان لری

مثال:- پر $\mathbb{N}$ (طبعي اعداد) بانه دي دالاندي دوه ګوني رابطه تعریف شویده

$$\odot: \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$$
$$(a,b) \longmapsto a\odot b = a^b$$

$(\mathbb{N},\odot)$ یو الجبري جوړښت (algebraic structure) دی. مګرتبدیلي خاصیت (commutative) نه لري . ځکه:

$$2\odot 3 = 2^3 = 8 \neq 9 = 3^2 = 3\odot 2$$

مثال 1.2:

(a) X یو سیت دی. پورسیت P(X) نظر د سیتو اتحاد او تقاطع ته یو الجبری ساختمان لري . یعني $(P(X),\cap)$ او $(P(X),\cup)$ الجبری جوړښت دي.

ځکه:

$$A,B\in P(X) \Rightarrow A,B\subseteq X \Rightarrow A\cup B\subseteq X \wedge A\cap B\subseteq X$$
$$\Rightarrow A\cup B\in P(X) \wedge A\cap B\in P(X)$$

(b): یو $M(2x2,\mathbb{R})$ سیت لاندي شکل لري

$$\mathrm{M:} = \{A\in M(2x2,\mathbb{R})\,|\,A = \begin{pmatrix} a & b\\ c & d\end{pmatrix}\ \}$$

(M,+) یوالجبری جوړښت (algebraic structure) دی. ځکه دمتریکسوخواصوله مخې لیکلی شو:

$$A, B \in M, A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \Rightarrow A + B \in M$$

$$-A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} \in M$$

(M,+) تبدیلي هم دی.

(M,.) هم یوالجبری جوړښت (algebraic structure) دی. ځکه دلته هم دمتریکسوخواصوله مخې لیکلی شو:

$$A,B \in M \Longrightarrow A.B \in M$$

مګر(M,.) تبدیلي خاصیت نه لري. ځکه:

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 2 & -2 \\ 2 & -1 \end{pmatrix} \in M$$

$$A.B = \begin{pmatrix} 1.2 + 2.2 & 1.(-2) + 2.(-1 \\ 2.2 + 1.2 & 2.(-2) + 1.(-1) \end{pmatrix} = \begin{pmatrix} 6 & -4 \\ 6 & -5 \end{pmatrix}$$

$$B.A = \begin{pmatrix} 2 & -2 \\ 2 & -1 \end{pmatrix} . \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ 0 & 3 \end{pmatrix}$$

لیدل کیږي چې $A.B \neq B.A$ دی

البته دلته "+„ دوه ګونې رابطه دمتریکسوجمع او ".„ دمتریکسوضرب دی. په عمومي ډول کولاې ووایو چې $M(nxn, \mathbb{R})$ سیت نظردمتریکسوجمع او ضرب ته الجبري جوړښت لري.

مثال 1.3:

(a) M:= $\{A \in M(2x2, \mathbb{R}) | A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a^2 + b^2 \neq 0\}$

(i)

$$\cdot : MxM \longrightarrow M$$
$$(A,B) \longmapsto A \cdot B$$

(M,.) یو الجبری جوړښت (algebraic structure) دی

(ii)

$$+ : MxM \longrightarrow M$$
$$(A,B) \longmapsto A+B$$

(M,+) ولي يو الجبرى جوړښت (algebraic structure) نه لري

حل (i) :

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in M$$

$$A.B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} . \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix}$$

$$(ac - bd)^2 + (ad + bc)^2 = (ac)^2 - 2\,acbd + (bd)^2$$

$$+ (ad)^2 + 2adbc + (bc)^2$$

$$= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2$$

$$a^2 + b^2 \neq 0 \;\wedge\; c^2 + d^2 \neq 0$$

$$\Longrightarrow (a^2 + b^2).(c^2 + d^2) \neq 0$$

$$\Longrightarrow (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 \neq 0$$

$$\Longrightarrow A.B \in M$$

يا په بله طريقه:

$$A,B \in M \Longrightarrow \det(A) = a^2 + b^2 \neq 0 \;\wedge\; \det(B) = c^2 + d^2 \neq 0$$

$$\det(A.B) = \det(A) . \det(B) \neq 0$$

$$\Longrightarrow (ac - bd)^2 + (ad + bc)^2 = \det(A.B) \neq 0$$

$$\Longrightarrow A.B \in M$$

په نتيجه کی (M, .) يو الجبرى جوړښت (algebraic structure) دی

حل (ii):

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in M$$

$$A+B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ -b - d & a + c \end{pmatrix}$$

که (M,+) یوالجبری جوړښت وي ، باید $A+B\in M$ صدق وکړی.

$(a+c)^2 + (b+d)^2 \neq 0$
$(a+c)^2 = a^2 + 2ac + c^2$
$(b+d)^2 = b^2 + 2bd + d^2$

د مثال په ډول د لاندي متریکسولپاره صدق نه کوی

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix} \in M$$

$$\mathrm{A + B} = \begin{pmatrix} 1-1 & 1-1 \\ -1+1 & 1-1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin \mathrm{M}$$

ځکه $0^2+0^2 = 0$ دی. په نتیجه کي (M,+) الجبری ساختمان نه دی .

تمرین 1.1:

(a) $M:= \{ a \in \mathbb{R} \mid -5\leq a \leq 3 \}$

ایا (M,+) یو الجبری جوړښت (ساختمان) لری

(b) که پر $\mathbb{R}$ باندی لاندي دوه ګونه رابطه تعریف شوی وی:

$$\oplus : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$
$$(a,b) \mapsto a \oplus b = \frac{1}{2} (a+b)$$

ثبوت کړی چي $(\mathbb{R}, \oplus)$ الجبري جوړښت لری. مګراتحادی خاصیت نه لری

(c) د $z = a + ib \in \mathbb{C}$ لپاره $|z| = \sqrt{a^2 + b^2}$ تعریف شویدی

$$G:= \{z\in \mathbb{C} \mid |z| = 1 \}$$

$$\cdot : G \times G \longrightarrow G$$
$$(z_1,z_2) \mapsto z_1 . z_2$$

ثبوت کړی چي (G,.) یوالجبري جوړښت (algebraic structure) دی

نوټ: عینیت عنصرپس له دي په e سره ښیو.

تعریف 3 . 1 : یو الجبری جوړښت (algebraic structure) $(G,\oplus)$ که د پورتنی تعریف (i) خاصیت ولری د semi group ، که (i),(ii) خواصه ولری د monoid اوکه (i),(ii) , (iii) خواصه ولری د ګروپ (group) په نوم یادیږی . که چیری په یوه ګروپ کی (iv) خاصیت هم صدق وکړی. بیا هغه

ته تبديلي گروپ (commutative group) ويل کيږی . يو تبديلي گروپ د ablean group په نوم هم ياديږی. که ديو گروپ دعناصروشميرمعين وي د معين گروپ (finite group) په نامه ياديږي. که هسی نه وي ورته غيرمعين گروپ (infinite Group) واي.

مثال: $(\mathbb{N},+)$ يو semi group دی. مګرځرنګه چې عينيت عنصر "0" په $\mathbb{N}$ کې شامل نه دی ، پس monoid نشي کيدای.

قضيه 1.1 : که $(G,\oplus)$ يو ګروپ وي. بيا :

(1) د هرعنصر $a \in G$ يوازی يوچپ معکوس (left-inverse) موجود دی چې داپه عين حال کی ښی معکوس (right-inverse) هم دی.

(2) يوازی يوچپ عينيت (left-identity) موجوددی، چې داپه عين حال کی ښی عينيت (right-identity) هم دی .

(1) **ثبوت** : که e چپ عينيت (left-identity او $\bar{a}$ چپ معکوس (left-inverse) د a په G کی وی. بايد ثبوت شی چې $\bar{a}$ ښی معکوس (right-inverse) د a هم دی. يعنې:

$$\bar{a}\oplus a = e \quad \Longrightarrow \quad a \oplus\bar{a} = e$$

ځرنګه چې G يو ګروپ دی ، پس د $\bar{a}$ دلپاره هم يوچپ معکوس $\bar{\bar{a}}$ موجود دی چې $\bar{\bar{a}}\oplus\bar{a} = e$ شی. يعنې :

$$\forall a \in G\ \exists\ \bar{a} \in G, \bar{a}\oplus a = e\ \wedge \exists\ \bar{\bar{a}} \in G, \bar{\bar{a}}\oplus\bar{a} = e$$

$a\oplus\bar{a} = e\oplus(a\oplus\bar{a})$ [ځکه e چپ عينيت دی]

$= (\bar{\bar{a}}\oplus\bar{a})\oplus(a\oplus\bar{a})$ [ځکه $\bar{\bar{a}}$ چپ معکوس د $\bar{a}$ دی]

$= \bar{\bar{a}}\oplus (\bar{a}\oplus(a\oplus\bar{a}))$ [اتحادی خاصيت]

$= \bar{\bar{a}} \oplus ((\bar{a}\oplus a)\oplus\bar{a})$ [اتحادی خاصيت]

$= \bar{\bar{a}}\oplus(e\oplus\bar{a})$ [ځکه $\bar{a}$ چپ معکوس د a دی]

$= \bar{\bar{a}} \oplus\bar{a}$ [ځکه e چپ عينيت دی]

$= e$ [ځکه $\bar{\bar{a}}$ چپ معکوس د $\bar{a}$ دی]

وښودل شوچې $\bar{a}$ ښی معکوس د a هم دی.

(2) ثبوت : که $e \in G$ چپ عينيت (left-identity) وی.

يعنې: $a = e\oplus a \quad \forall a \in G$

باید ثبوت شی: $a = a\oplus e \quad \forall a \in G$

$a \in G \implies \exists\ \bar{a} \in G\ ;\ \bar{a}\oplus a = e$

$a\oplus e = a\oplus(\bar{a}\oplus a)$

$= (a\oplus\bar{a})\oplus a$ [اتحادی خاصیت]

$= e\oplus a$ [(1) ته نظر]

$= a$ [ځکه e چپ عینیت دی]

ولیدل شول چې e ښی عینیت (right-identity) هم دی

مونږ.فرض کووچې $\bar{e} \in G$ هم یو عینیت د G دی

$e\oplus\bar{e} = e$ [ځکه $\bar{e}$ عینیت دی]

$e\oplus\bar{e} = \bar{e}$ [ځکه e عینیت دی]

په نتیجه کی $e = \bar{e}$

ثبوت شو چې په یوه گروپ کی فقط یو دعینیت عنصر(identity) موجود دی

فرض کوو چې د $\bar{a}$ پرعلاوه $a' \in G$ هم یو معکوس د a دی.

$a' = a'\oplus e$ [ځکه e عینیت دی]

$= a'\oplus(a\oplus\bar{a})$ [ځکه $\bar{a}$ معکوس د a دی]

$= (a'\oplus a)\oplus\bar{a}$ [اتحادی خاصیت]

$= e\oplus\bar{a} = \bar{a}$ [ځکه a' معکوس د a دی]

ولیدل شول چې په یوه گروپ کی دهرعنصرلپاره فقط یوازی یومعکوس (inverse) موجود دی

نوټ: څرنگه چې دیو a عنصر چپ معکوس په عین حال کی ښی معکوس هم دی. مونږ پس له دی هغه ته معکوس (inverse) وایو او په a^{-1} ښیوو. همدارنگه د عینیت عنصر (identity) لپاره.

مثال: $(\mathbb{R},+), (\mathbb{Q},+), (\mathbb{Z},+)$ تبدیلی گروپونه دي چې د عنیت عنصریې صفر „0" او -a معکوس د a دی .

$(\mathbb{R}^*,.), (\mathbb{Q}^*,.)$ تبدیلی گروپونه دي چې د عنیت عنصریې یو „1" او

$a^{-1} = \frac{1}{a}$ معکوس دی a دی. ځکه $a.\frac{1}{a} = 1$ کیږی

مثال 1.4: که مونږ د $M:= M(2x2,\mathbb{R})$ سیت په نظرکې ونیسو. پوهیږوچې (M,+) او (M,.) الجبري جوړښت (ساختمان) لري. M نظرد متریکسوجمع اوضرب ته monoid دی. ځکه دمتریکسودخواصوله مخې لیکلی شو:

اتحادي خاصيت (associativity):

A,B,C∈ M

$A+(B+C) = (A+B)+C \wedge A.(B.C) = (A.B).C$

عينيت عنصر: صفرمتريکس د (M,+) عينيت عنصر اوواحد متريکس د (M,.) عينيت عنصر دی. يعنې:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} , \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \quad G$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+0 & b+0 \\ c+0 & d+0 \end{pmatrix} = A$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+0 & 0+b \\ c+0 & 0+d \end{pmatrix} = A$$

(M,+) ګروپ هم دی. ځکه:

$$-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

$$A+(-A) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} = \begin{pmatrix} a-a & b-b \\ c-c & d-d \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

وليدل شوچې $-A$ معکوس د A دی

د متريکسو دخواصو په اساس (M,+) تبديلي ګروپ دی

مګر (M,.) ګروپ نه دی. ځکه صفرمتريکس معکوس نه لري. همدارنګه دمثال په ډول دالاندي متريکس معکوس نه لري

$$A = \begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix}$$

د (M,+) او (M,.) پورتني خواص نه يوازی د $M(2x2, \mathbb{R})$ لپاره بلکه په عمومي صورت د $M(nxn, \mathbb{R})$ لپاره هم صدق کوي.

نوټ1.1: دموهومی اویا مختلط اعدادو (complex number) سیت په $\mathbb{C}$ سره ښودل کیږی او هر $z\in \mathbb{C}$ د $z=a+ib$ شکل لری. چې دلته $a,b \in \mathbb{R}$ دي.

a = real part , i = imaginary unit , b = imaginary part ,

absolute value:= $|z| = \sqrt{a^2 + b^2}$

complex conjugate:= $\bar{z}$ = a – ib

$(\mathbb{C},+)$ يو تبديلی گروپ دی. چې عنيت عنصريي صفر "0" او -z=-a-ib معکوس د z=a+ib دی

$(\mathbb{C}^*,.)$ هم يو تبديلی گروپ دی. چې عنيت عنصريي "1" دی. معکوس د $z=a+ib \in \mathbb{C}^*$ که z^{-1} وی په لاندي شکل لاس ته راځي

$$z^{-1} = \frac{1}{z} = \frac{1}{a+ib} = \frac{1}{a+ib}.\frac{a-ib}{a-ib} = \frac{a-ib}{a^2 + iab - iab - i^2 b^2}$$

$$= \frac{a-ib}{a^2 - (-1) b^2} = \frac{a-ib}{a^2 + b^2} = \frac{\bar{z}}{|z|^2}$$

$$z.\, z^{-1} = \frac{z.\bar{z}}{|z|^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1$$

ليدل کيږی چې z^{-1} معکوس د z دی. دگروپ نور خواصونه هم صدق کوی.

مثال: $z = 2\text{-}i3 \in \mathbb{C}^*$. غواړو په $(\mathbb{C}^*,.)$ گروپ کی معکوس د z پيدا کړو.

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{2+i3}{2^2 + (-3)^2} = \frac{2+i3}{4+9} = \frac{2+i3}{13} = \frac{2}{13} + \frac{3}{13}i$$

ليدل کيږی چې:

$$z.z^{-1} = (2 - 3i).\left(\frac{2+i3}{13}\right) = \frac{(2-3i).(2+i3)}{13} = \frac{4-9(i.i)}{13}$$

$$= \frac{4-9(-1)}{13} = \frac{13}{13} = 1$$

په نتيجه کی $z^{-1} = \frac{2+i3}{13}$ معکوس د $z = 2 - 3i$ دی

تمرين: معکوس د $z = -3+5i \in \mathbb{C}^*$ نظر $(\mathbb{C},+)$ او $(\mathbb{C}^*,.)$ ته پيداکړی

تعريف 1.4: مونږيو معين سيت $\{ a_1, a_2, a_3, ... , a_n \}$ =: G لرو. که

$(G,*)$ یو گروپ او a_1 دهغه عینیت عنصر (identity) وی، بیا کولای شوهغه په یو جدول کی په لاندي ډول وښیو:

*	a_1	a_2	a_3	.	.	.	.	.	a_n
a_1	$a_1* a_1$	$a_1* a_2$	$a_1* a_3$	.	.	.	.	.	a_1*a_n
a_2	$a_2* a_1$	$a_2* a_2$	$a_2* a_3$	.	.	.	.	.	a_2*a_n
a_3	$a_3* a_1$	$a_3* a_2$	$a_3* a_3$	.	.	.	.	.	a_3*a_n
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
a_n	$a_n * a_1$	$a_n * a_2$	$a_n * a_3$	.	.	.	.	.	$a_n * a_n$

په پورتنی جدول کی باید په هره لیکه (همدارنگه په هره ستنی (ستون)) کی فقط تنها مختلف عناصرد G ویی. دا ډول جدول د Cayley Table په نوم یادیږی.
یو Cayley جدول هغه وخت گروپی جوړښت لری، چې جدول یی لاندي خواص ولری:

(i) عینت عنصر موجود وي
(ii) چپ او ښی معکوس سره مساوی وي
(iii) اتحادی خاصیت ولرې

مثال: G:={a,b,c,d,e}

*	a	b	c	d	e
a	a	b	c	d	e
b	b	a	d	e	c
c	c	d	e	a	b
d	d	e	b	c	a
e	e	c	a	b	d

په پورتني جدول کې د عيتيت عنصر a دی. مګر $(G, *)$ ګروپ نه دی. خکه

$c * d = a \neq b = d * c$

د c چپ معکوس d دی، مګرهغه ښی معکوس نه دی

مثال : $A^{(2)} := \{e, a\}$. مونږکولای شو $A^{(2)}$ نظر $\odot$ دوه ګوني رابطی له مخي په لاندي شکل په Cayley Table کی وښیو

$\odot$	e	a
e	e	a
a	a	e

$e \odot e = e \ , e \odot a = a = a \odot e \quad , a \odot a = e$

$(A^{(2)}, \odot)$ یوتبدیلی ګروپ دی

تمرين 1.2

(a) ولی $(\mathbb{N}, +), (\mathbb{Z}, .)$ او $(\mathbb{R}, .)$ ګروپی ساختمان نه لری.

(b) ثبوت کړی چي $(\mathbb{Q}^*, .)$ يو ګروپ دی.

(c) $G := \{1, -1\}$. ثبوت کړی چي G نظرضرب ته يو ګروپ دی

اودهغه Cayley جدول څه شکل لری

(d) $G:=\{-1,1,i,-i\} \subset \mathbb{C}$. ثبوت کړی چي G نظرضرب ته يو ګروپ دی اودهغه Cayley جدول څه شکل لری

مثال 1.4 : د $A^{(4)}=\{a_0,a_1,a_2,a_3\}$ پرسيت باندی یوه „$\oplus$" دوه ګوني رابطه په لاندي شکل په یو Cayley جدول کی تعریف شویده :

په پورتنی جدول کي $\oplus$ دوګونه رابطه په لاندي ډول عمل کوي:

$\oplus$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

په پورتنی جدول کې ⊕ دوګونه رابطه په لاندې ډول عمل کوي:

$$a_\lambda \oplus a_\mu = \begin{cases} a_{\lambda+\mu} & if \quad \lambda+\mu < 4 \\ a_{\lambda+\mu-4} & if \quad \lambda+\mu \geq 4 \end{cases}$$

$(A^{(4)}, \oplus)$ یو ګروپ دی.ځکه:

(1) اتحادی (associativity) ($\lambda,\mu,\nu \in \mathbb{N}$ و $0 \leq \lambda,\mu,\nu \leq 3$)

$$(a_\lambda \oplus a_\mu) \oplus a_\nu = \begin{cases} a_{\lambda+\mu} \oplus a_\nu & if \quad \lambda+\mu < 4 \\ a_{\lambda+\mu-4} \oplus a_\nu & if \quad \lambda+\mu \geq 4 \end{cases}$$

$$= \begin{cases} a_{\lambda+\mu+\nu} & if \quad \lambda+\mu+\nu < 4 \\ a_{\lambda+\mu+\nu-4} & if \quad 4 \leq \lambda+\mu+\nu < 8 \\ a_{\lambda+\mu+\nu-8} & if \quad \lambda+\mu+\nu \geq 8 \end{cases}$$

عین نتیجه لاس ته راځی ، که مونږ $a_\lambda \oplus (a_\mu \oplus a_\nu)$ په پام کی ونیسو .

پس لهذا:

$$a_\lambda \oplus (a_\mu \oplus a_\nu) = (a_\lambda \oplus a_\mu) \oplus a_\nu$$

(2) a_0 د عینیت عنصر (identiy) دی

(3) معکوس (inverse) : د هر a_λ یو عنصر a_μ معکوس دهغه دی ، پدی شرط چې $\mu + \lambda = 4$ شی. دمثال په ډول : $a_1 \oplus a_3 = a_0$

مثال 1.3 : د $A^{(2,2)} :=\{b_1,b_2,b_3,b_4\}$ پرسیت باندی یوه „⊙" دوه ګونه رابطه په لاندې شکل په یو Cayley جدول کی تعریف شویده :

⊙	b_1	b_2	b_3	b_4
b_1	b_1	b_2	b_3	b_4
b_2	b_2	b_1	b_4	b_3
b_3	b_3	b_4	b_1	b_2
b_4	b_4	b_3	b_2	b_1

په جدول کی لیدل کیږی چې b_1 دعینیت عنصردی او هرعنصرخپله معکوس هم دی .ځکه:

$$b_2 \odot b_2 = b_3 \odot b_3 = b_4 \odot b_4 = b_1$$

د $\lambda, \mu, \nu \in \mathbb{N}$ لپاره چې $2 \le \lambda, \mu, \nu \le 4$ او λ, μ , ν مختلف وی ، پورتنی دوه ګونې رابطه (binary operation) په لاندې ډول تعریف شوی ده.

$$b_\lambda \odot b_\mu = b_\nu$$

اتحادی(associativity) :

د $\lambda, \mu, \nu \in \mathbb{N}$ چې $2 \le \lambda, \mu, \nu \le 4$ او λ, μ , ν مختلف وی.
بیا لیکلی شو:

$$\left(b_\lambda \odot b_\mu\right) \odot b_\nu = b_\nu \odot b_\nu = b_1$$
$$b_\lambda \odot \left(b_\mu \odot b_\nu\right) = b_\lambda \odot b_\lambda = b_1$$
$$\left(b_\lambda \odot b_\lambda\right) \odot b_\lambda = b_1 \odot b_\lambda = b_\lambda$$
$$b_\lambda \odot \left(b_\lambda \odot b_\lambda\right) = b_\lambda \odot b_1 = b_\lambda$$
$$(b_\mu \odot b_\mu) \odot b_\nu = b_1 \odot b_\nu = b_\nu$$
$$b_\mu \odot \left(b_\mu \odot b_\nu\right) = b_\mu \odot b_\lambda = b_\nu$$
$$(b_\mu \odot b_\nu) \odot b_\nu = b_\lambda \odot b_\nu = b_\mu$$
$$b_\mu \odot (b_\nu \odot b_\nu) = b_\mu \odot b_1 = b_\mu$$
$$(b_\mu \odot b_\nu) \odot b_\mu = b_\lambda \odot b_\mu = b_\nu$$
$$b_\mu \odot \left(b_\nu \odot b_\mu\right) = b_\mu \odot b_\lambda = b_\nu$$

په نتیجه کی ثبوت شو، چې $(A^{(2,2)}, \odot)$ یو ګروپ دی. $A^{(2,2)}$ ګروپ د Klein four-group(F.Klein 1849-1925) په نوم یادیږی.

لیما 1.1: $(G, \oplus)$ یو ګروپ دی. د هردو $a, b \in G$ عنصرولپاره لاندې معادله صدق کوی :

$$(a \oplus b)^{-1} = b^{-1} \oplus a^{-1}$$

ثبوت: باید ثبوت شی چې $a^{-1}\oplus b^{-1}$ هم معکوس د $a\oplus b$ دی. یعني باید ثبوت شی چې:

$$(b^{-1}\oplus a^{-1})\oplus(a\oplus b) = e$$

$$(b^{-1}\oplus a^{-1})\oplus(a\oplus b) = b^{-1}\oplus\left(a^{-1}\oplus(a\oplus b)\right)$$ [خاصیت اتحادی]

$$= b^{-1}\oplus((a^{-1}\oplus a)\oplus b)$$

$$= b^{-1}\oplus(e\oplus b) = b^{-1}\oplus b = e$$

$$\Longrightarrow (a\oplus b)^{-1} = b^{-1}\oplus a^{-1}$$

قضیه 1.2: که $(G,\oplus)$ یوګروپ او $e\in G$ دهغه عینیت عنصروی. بیا دالاندي افادی صدق کوی:

(1) $a,b,c\in G$

$$c\oplus a = c\oplus b \Rightarrow a = b$$

$$\wedge$$

$$a\oplus c = b\oplus c \Rightarrow a = b$$

یعني په یوه ګروپ کی اختصارول امکان لری .

(2)

$$a,b\in G\ ,\ \exists!\, x\in G\ ;\ \ x\oplus a = b \quad \wedge \quad \exists!\, y\in G\ ; a\oplus y = b$$

ثبوت (1): مونږفرض کوچې $c\oplus a = c\oplus b$ ده

$$c\oplus a = c\oplus b \Rightarrow c^{-1}\oplus(c\oplus a) = c^{-1}\oplus(c\oplus b)$$

$$\Rightarrow (c^{-1}\oplus c)\oplus a = (c^{-1}\oplus c)\oplus b$$

$$\Rightarrow e\oplus a = e\oplus b$$

$$\Rightarrow a = b$$

همدارنګه کولای شوثبوت کړوچې:

$$a\oplus c = b\oplus c \Rightarrow a = b$$

ثبوت(2):

$$a,b\in G \Rightarrow \exists a^{-1}\in G$$ [ځکه G یو ګروپ دی]

$$\Rightarrow \ b\oplus a^{-1}\in G$$

که مونږ $x := b\oplus a^{-1}$ وضع کړو. پدی صورت:

$$x = b\oplus a^{-1} \Rightarrow x\oplus a = (b\oplus a^{-1})\oplus a = b\oplus(a\oplus a^{-1})$$

$$= b\oplus e = b$$

ولیدل شول چې هغه ډول یو x په G کی موجود دی .

که $w\in G$ هم همغه ډول یو عنصروی. یعني $w\oplus a = b$

$$w \oplus a = b \Rightarrow (w \oplus a) \oplus a^{-1} = b \oplus a^{-1}$$
$$\Rightarrow w \oplus (a \oplus a^{-1}) = b \oplus a^{-1}$$
$$\Rightarrow w \oplus e = b \oplus a^{-1} \quad \Rightarrow w = b \oplus a^{-1} = x$$

ثبوت شوچې فقط یوازی یو x په هغه خاصیت وجودلری.

قضیه 1.3: که $\oplus$ یوه دوه گونه رابطه پریوه سیټ $G \neq \emptyset$ وي. بیا دالاندي افادی له یوبل سره معادل دي:

(1) $(G,\oplus)$ یو گروپ دی

(2)

(a) $\oplus$ اتحادی خاصیت لری

(b) د هر دو عنصرو $a, b \in G$ لپاره $x, y \in G$ دلاندي خواصوسره وجود لري:

$$x \oplus a = b \;\; \wedge \;\; a \oplus y = b$$

ثبوت:

(1) $\Rightarrow$ (2) : گروپ د خواصو اود 1.2 قضیې څخه لاس ته راځی.

(2) $\Rightarrow$ (1) : نظر په (b) کولای شوولیکو:

$c \in G \Rightarrow \exists e \in G\, ; e\oplus c = c$ [که c = a = b وی]

$a \in G \Rightarrow \exists y \in G\, ; c\oplus y = a$

$$\Rightarrow e\oplus a = e\oplus(c\oplus y)$$
$$= (e \oplus c) \oplus y = c \oplus y = a$$

پس دعینیت عنصر e موجود دی.

$e, a \in G \Rightarrow \exists x \in G\, ; x\oplus a = e$

یعني x معکوس د a دی.

مثال 1.5 :

$$G := \{A \in M(2x2,\mathbb{R}) \,|\, A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a^2 + b^2 \neq 0\}$$

$\cdot : G \times G \longrightarrow G$

$(A,B) \longmapsto A\cdot B$

(G,.) یو گروپ دی

حل: په 1.3 مثال کی مو ولیدل چې (G,.) یو الجبری جوړښت (ساختمان) لري.
څرنگه چې $(M(2x2,\mathbb{R})\, , .)$ اتحادي خاصیت لری . پس (G,.) هم اتحادي خاصیت لری.ځکه $G \subseteq M(2x2,\mathbb{R})$

عینیت عنصر یې واحد متریکس دی. ځکه:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G \ , \ A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \ G$$

$$A.E = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+0 & 0+b \\ -b+0 & 0+a \end{pmatrix} = A$$

معکوس عنصر:

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \ G$$

د A معکوس متریکس لاندي شکل لري:

$$A^{-1} = \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in G$$

ځکه:

$$A^{-1} = \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}$$

$$(\frac{a}{a^2+b^2})^2 + (\frac{-b}{a^2+b^2})^2 = \frac{a^2}{(a^2+b^2)^2} + \frac{b^2}{(a^2+b^2)^2} = \frac{a^2+b^2}{(a^2+b^2)^2}$$

$$a^2 + b^2 \neq 0 \Rightarrow \frac{a^2+b^2}{(a^2+b^2)^2} \neq 0 \ \Rightarrow \ A^{-1} \in G$$

$$A \cdot A^{-1} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} . \ \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

$$= \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a^2+b^2 & -ab+ab \\ -ab+ab & a^2+b^2 \end{pmatrix}$$

$$= \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix}$$

$$= \frac{a^2+b^2}{a^2+b^2} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ثبوت شو چې (G,.) یو ګروپ دی

مثال 1.6 :

$$GL(2, \mathbb{R}) := \{ A \in M(2 \times 2, \mathbb{R}) \mid A \text{ invertible (معکوس پذیر) } \}$$

(GL(2, ℝ) ,.) یو ګروپ دی چې عینیت عنصریې واحد متریکس E_2 دی.

حل: ($GL(2, \mathbb{R})$, .) یوالجبری جوړښت (algebraic structure) لری.
ځکه د خطی الجبرله مخی:

$$A,B\in GL(2,\mathbb{R}) \Rightarrow \det(A.B) = \det A . \det B \neq 0$$
$$\Rightarrow \exists D \in GL(2,\mathbb{R}) ; D = (A.B)^{-1}$$
$$\Rightarrow A.B\in GL(2,\mathbb{R})$$
$$A\in GL(2,\mathbb{R}) \Rightarrow \det A \neq 0 \Rightarrow \exists A^{-1}\in GL(2,\mathbb{R}) ; A. A^{-1} = E_2$$

په نتیجه کی ($GL(2, \mathbb{R})$, .) یو ګروپ دی.

نوت: کولای شو په عمومی ډول ثبوت کړوچې ($GL(n, \mathbb{R})$, .) یو ګروپ دی.
البته n دلته یو طبعی عدد دی.

تمرین 1.3: $G := \{z \in \mathbb{C} \mid |z|= 1\}$ اود z=a+ib لپاره $|z|$ په دي ډول
تعریف شوی دی: $|z| = \sqrt{a^2 + b^2}$

پر G باندي لاندي دوه ګونه رابطه لرو:

$$\cdot : G \times G \longrightarrow G$$
$$(z_1,z_2) \longmapsto z_1 . z_2$$

ثبوت کړی چی (G,.) یو ګروپ دی

نوت : مونږپس له دی یوه دوه ګونه رابطه *(Binary operation)* په "·" سره
ښیواوهدف دلته دعادی ضرب عملیه نه ده.

مثال 1.7 : د $D_4 := \{e, a, b, c, d, f, g, h\}$ پرسیت باندی یوه دوه ګوني رابطه
(Binary operation) په یوکیلی جدول کی په لاندي شکل تعریف شویده :

.	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	h	g	f	e	c	b	a
f	f	d	h	g	a	e	c	b
g	g	f	d	h	b	a	e	c
h	h	g	f	d	c	b	a	e

(D$_4$,.) یو ګروپ دی چې عینیت عنصریې e دی . څرنګه چې a.c=e دی پس معکوس د a د c عنصر دی. یعنې $a^{-1} = c$ او څرنګه چې h .h = e دی پس معکوس د h خپله h دی . یعنې $h^{-1} = h$.په همدی ډول کولای شو د جدول له مخې د ټولو عناصرو معکوس پیداکړو .

اتحادی خاصیت (assosativity) هم صدق کوی . د مثال په ډول:

a. (d . f)= a . c =e

(a . d). f = f . f = e

همدی ډول کولای شودټولوعناصراتحادی خاصیت وښیو.

(D$_4$,.) ګروپ د Dihedral group په نوم یادیږی .

مثال 1.8: Q_8:={ e,a,b,c,d,f,g,h} نظر لاندینی کیلی جدول (cayley table) ته یوګروپ دی .

.	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	a	e	g	h	f	d
c	c	b	e	a	h	g	d	f
d	d	f	h	g	a	e	b	c
f	f	d	g	h	e	a	c	b
g	g	h	d	f	c	b	a	e
h	h	g	f	d	b	c	e	a

e عینیت عنصر (identety) د Q_8 دي. مګرتبدیلی نه دی.ځکه

$$d.b = h \neq g = b.d$$

مثال 1.9 : Q_6:={ e,a,b,c,d,f } هم نظرلاندنی کیلی جدول (cayley table) له مخې یو ګروپ دی .

.	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

نوټ: لاندي گروپونه معين دي:

$A^{(2)}, A^{(4)}, A^{(2,2)}, D_4, Q_8, Q_6$

$|A^{(2)}| = 2$, $|A^{(4)}| = |A^{(2,2)}| = 4$, $|Q_6| = 6$, $|D_4| = |Q_8| = 8$

تمرين 1.4 :

(a) $G=\{ e,a,b \}$ او $\cdot : G\text{x}G \to G$ يوه دوه گونه رابطه ده . لاندي جدول داډول تکميل کړی چي $(G, \cdot)$ يوگروپ شی .

.	e	a	b
e	e	a	b
a	a		e
b	b	e	

(b) $G=\{ e,a,b,c \}$ او $\cdot : G\text{x}G \to G$ يوه دوه گونه رابطه ده .
لاندي جدول داډول تکميل کړی چي $(G,.)$ يو گروپ شی .

.	e	a	b	C
e	e	a	b	c
a	a		e	b
b	b	e		
c	c	b		

(c) د $A^{(2,2)}$, $A^{(4)}$, D_4 , Q_6 او Q_8 په گروپونوکی کوم يو تبديلی نه دی

تمرين 1.5 : $(G,\oplus)$ يو گروپ چي عينيت عنصری $e \in G$ دی . ثبوت کړی :

$$a \in G; a\oplus a = a \Rightarrow a = e$$

(يعني په يوه گروپ کي که يو عنصرپورتنی خاصيت ولري. هغه عينيت عنصردی)

تمرين 1.6 : پر $\mathbb{R}$ (حقيقی اعداد) لاندي دوه گونه رابطه تعريف شوی ده :

$$\odot : \mathbb{R} \text{ x } \mathbb{R} \longrightarrow \mathbb{R}$$
$$(a,b) \longmapsto a \odot b = \frac{1}{2}(a+b)$$

ثبوت کړی چې ولی $(\mathbb{R}, \odot)$ ګروپ کیدای نه شي

مثال 1.10 : که مونږ لاندي متریکسونه ولرو:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} , K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$Q: = \{\pm E , \pm I , \pm J , \pm K\}$$

البته دلته د هرمتریکس منفی لاندي شکل لري:

$$-E=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} , \quad -I =\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} ,$$

$$-J=\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} , \quad -K=\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$\cdot : Q \times Q \longrightarrow Q$$

$$(A,B) \longmapsto A\cdot B$$

په اسانه ښودل کیدای شی چی " · " یوه دوه ګونه رابطه (binary operation) ده او E دهغه عینیت عنصردی . دهر $A \in Q \setminus \{\pm E\}$ لپاره $-A$ دهغه معکوس اود $-E$ معکوس خپله $-E$ دی

اتحادي خواص هم صدق کوي. په نتیجه کی (. , Q) یوګروپ دی. مګر تبدیلي نه دی ځکه:

$$I.J = K , J.I = -K \Rightarrow I.J \neq J.I$$

د کیلی جدول (caley table) یی دالاندي شکل لري

.	E	-E	I	-I	J	-J	K	-K
E	E	-E	I	-I	J	-J	K	-K
-E	-E	E	-I	I	-J	J	-K	K
I	I	-I	-E	E	K	-K	-J	J
-I	-I	I	E	-E	-K	K	J	-J
J	J	-J	-K	K	-E	E	I	-I
-J	-J	J	K	-K	E	-E	-I	I
K	K	-K	J	-J	-I	I	-E	E
-K	-K	K	-J	J	I	-I	E	-E

تمرین 1.7 : ایا { 0,1,2 } = G نظر جمع او ضرب ته ګروپی جوړښت لری.

تمرین 1. 8 : $D_6 = \{a,b,c,x,y,z\}$ او " . " یوه دوه ګونه رابطه پر D_6 باندی ده. لاندي جدول داډول تکمیل کړی چې (D_6 , .) یو ګروپ شی.

.	a	b	c	x	y	Z
a					c	b
b		x	z			
c		y				
x				x		
y						
z		a			x	

مثال 1.11: مونږ.لاندي متریکسونه لرو:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} , B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
$$C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$Q_4 := \{E,A,B,C\}$

$$. : Q_4 \times Q_4 \rightarrow Q_4$$
$$(X,X) \mapsto X.Y$$

Q_4 یو ګروپ دی او کیلی جدول (caley table) یی لاندي شکل لري:

.	E	A	B	C
E	E	A	B	C
A	B	E	C	B
B	B	C	A	E
C	C	B	E	A

تعریف 1.5: (G,.) یو الجبری جوړښت (algeb-struct) او $a\in G$.

$\tau_a : G \to G$
$x \mapsto a.x$

${}_a\tau : G \to G$
$x \mapsto x.a$

د τ_a right-translation او ${}_a\tau$ د left-translation په نوم یادیږي

لیما 1.2: (G,.) یو الجبری جوړښت (algeb-struct) دی. بیا :

(1) که (G,.) یو گروپ وي. په دي صورت دهر $a \in G$ لپاره τ_a یو bijective دی

(2) که (G,.) اتحادی (associativity) خاصیت ولری او دهر $a \in G$ لپاره τ_a surjective وي. په دي صورت (G,.) یو گروپ دی .

ثبوت (1)

$b \in G \Rightarrow \exists! \ x \in G$; a.x = b [د 1.2 قضیې له مخې]

$\Rightarrow \tau_a(x) = b \Rightarrow \tau_a$ surjective

x,y$\in G$; $\tau_a(x) = \tau_a(y)$
$\Rightarrow$ a.x = a.y $\Rightarrow$ x = y [د 1.2 قضیې له مخې]
$\Rightarrow \tau_a$ injecetiv

ثبوت شو چې τ_a بایجکتیف دی

ثبوت (2)

$a \in G$
$\Rightarrow \exists \ x \in G$; $\tau_a(x) =$ a.x = a [surjective یو τ_a ځکه]

د a.x = a څخه نتیجه کیږي چی یود عینیت عنصر e:= x موجود دی. پس

$e \in G \Rightarrow \exists \ y \in G$; $\tau_a(y) =$ a.y = e [surjective یو τ_a ځکه]

د a.y = e څخه نتیجه کیږي چی یو معکوس د a لپاره موجود دی. پس ثبوت شوچی (G,.) یو گروپ دی . پورتنی لیما د ${}_a\tau$ لپاره هم صدق کوي

تبصره: (G, ∗) یو گروپ دی . د پورتنی لیما څخه نتیجه اخلوچي د هر $a \in G$ لپاره دالاندي تابع bijecktive دي

f: $G \longrightarrow$ G   f: $G \longrightarrow$ G
$x \longmapsto a * x$ $x \longmapsto a * x$

دمثال په ډول د $(\mathbb{Z}, +)$ او $(\mathbb{R}^*, .)$ په ګروپونوکې دالاندي تابع bijective دي

$f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ $\qquad$ $f : \mathbb{Z} \longrightarrow \mathbb{Z}$

$x \longmapsto \frac{2}{3} \cdot x$ $\qquad$ $x \longmapsto 5 + x$

مثال 1.12:

$\odot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

$(a,b) \longmapsto a \odot b = a + b + 3$

غواړوثبوت کړو چې $(\mathbb{R}, \odot)$ یو ګروپ دی

حل: لیدل کیږی چې $(\mathbb{R}, \odot)$ یو الجبري جوړښت (ساختمان) لری

اتحادي خاصیت:

$a,b,c \in \mathbb{R}$

$(a \odot b) \odot c = (a+b+3) \odot c = a+b+c+6$

$= a + b \odot c + 3 = a \odot (b \odot c)$

عینیت عنصر: که e عینیت عنصروی. پس باید:

$\forall a \in \mathbb{R} ; a \odot e = a \Longrightarrow a + e + 3 = a \Longrightarrow e = -3$

یعني عینیت عنصر $e = -3$ دی

معکوس عنصر (inverse element) : که b معکوس د a وي. پس باید:

$a \odot b = -3 \Longrightarrow a + b + 3 = -3 \Longrightarrow b = -a - 6 = -(a+6)$

(a+6) معکوس د a دی. ځکه:

$a \odot (-a - 6) = a - a - 6 + 3 = -3 = e$

په نتیجه کی $(\mathbb{R}, \odot)$ یو ګروپ دی

تمرین 1.10:

$\odot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

$(a,b) \longmapsto a \odot b = a + b + 5$

ثبوت کړی $(\mathbb{R}, \odot)$ یو ګروپ دی

دویم فصل

گروپ هومورفیزم

(Group Homomorphism)

تعریف 2.1 : $(G,\oplus)$ او $(G',\odot)$ دوه گروپه دي. یو mapping $\varphi: G \longrightarrow G'$ دلاندي خواصو سره د Group Homomorphism (G - Hom) په نوم یادیږي.

$(a \oplus b) = \varphi(a)\odot\varphi(b) \quad (\quad \forall a,b \in G \quad)$

یو G-Hom چې injective وي، ورته Group Monomorphism (G-Monom)، که surjective وي ورته Group Epimorphism (G-Epim) او که bijective وی بیا ورته Group Isomorphism (G-Isom) ویل کیږي.

تعریف 2.2 : $(G,\oplus)$ یوگروپ دی. که $\varphi: G \longrightarrow G$ یو G-Hom وی، بیا ورته Group Endomorphism (G-Endo) ویل کیږی. یو G-Endo چې bijective هم وي د Group Automorphism (G-Auto) په نوم یادیږي.

مثال :

$$\varphi \ : (\mathbb{R},+) \longrightarrow (\mathbb{R},+)$$
$$x \quad \longmapsto \quad 2x$$

مونږپوهیږوچې د حقیقی اعدادو سیټ $\mathbb{R}$ نظرجمع "+" ته یو گروپ دی.

$x,y \in \mathbb{R}$

$\varphi(x+y) = 2(x+y) = 2x + 2y = \varphi(x) + \varphi(y)$

$\Rightarrow \ \varphi$ G-Hom

څرنگه چې φ اینجکتیف او سورجیکتیف دی . پس G-Monom او G-Epim هم دی. په نتیجه کي یو G-Isom دی.

که φ په لاندي ډول تعریف شي :

$$\varphi \ : (\mathbb{Z},+) \longrightarrow (\mathbb{Z},+)$$
$$x \quad \longmapsto \quad 2x$$

مونږپوهیږوچي د تام اعدادو سیټ $\mathbb{Z}$ نظرجمع "+" ته یو ګروپ دی. لیدل کیږي چې φ انجکتیف او G-Hom ده. پس یو G-Monom دی.
مګر φ سورجکتیف نه ده . پس G-Epim هم نشي کیدای. ځکه دمثال په ډول د -1 لپاره هیڅ تام عدد x نه پیداکیږی ، چه $(-1 = \varphi(x)$ شی.
که φ په لاندي ډول تعریف شي :

$$\varphi : (\mathbb{R}^*, .) \to (\mathbb{R}^*, .)$$
$$x \mapsto 2x$$

مونږپوهیږوچي $\mathbb{R}^*$ (د حقیقی اعدادو سیټ بی له صفر) نظرضرب "." ته یو ګروپ دی .

$x,y \in \mathbb{R}^*$

$$\varphi(x.y) = 2(x\,.\,y) = 2x.y \neq 2x\,.2y = \varphi\,(x)\,.\,\varphi(y)$$

ولیدل شول چې φ یو G-Hom نه دی
که φ په لاندي ډول تعریف شي :

$$\varphi : (\mathbb{R}^*, .) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto 2x$$

$x,y \in \mathbb{R}^*$

$\varphi(x.y) = 2(x\,.\,y) = 2x.y \quad \wedge \quad \varphi(x) + \varphi(y) = 2x + 2y$

$\Rightarrow \quad \varphi(x.y) \neq \varphi(x) + \varphi(y)$

معلوم شوچې φ یو G-Hom نه دی
که φ په لاندي ډول تعریف شي :

$$\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto -x$$

$x,y \in \mathbb{R}$

$\varphi(x+y) = -(x + y) = -x - y = \varphi(x) + \varphi(y) \Rightarrow \varphi$ G-Hom

که φ په لاندي ډول تعریف شي :

$$\varphi : (\mathbb{R}^*, .) \longrightarrow (\mathbb{R}^*, .)$$
$$x \longmapsto -x$$

$x,y \in \mathbb{R}^*$

$\varphi(x.y) = -x.y \quad \wedge \quad \varphi(x) . \varphi(y) = (-x) . (-y) = x.y$

$\Rightarrow \quad \varphi(x.y) \neq \varphi(x) . \varphi(y)$

په نتیجه کی φ یو G-Hom نه دی

نوټ 2.1: په عمومي صورت کولای شو ووایو چې:

(a) د هر $a \in \mathbb{R}$ لپاره دا لاندي تابع یو G-Isom ده

$$\varphi : (\mathbb{R},+) \longrightarrow (\mathbb{R},+)$$
$$x \mapsto ax$$

(b) د هر $m \in \mathbb{Z}$ لپاره دا لاندي تابع یو G-Monom دی

$$\varphi : (\mathbb{Z},+) \longrightarrow (\mathbb{Z},+)$$
$$x \mapsto mx$$

مثال: دا لاندي Exponentialfunction یو G-Isom دی

$$\exp : (\mathbb{R},+) \longrightarrow (\mathbb{R}_+^*,.)$$
$$x \mapsto e^x$$

: G-Hom

$x,y \in \mathbb{R}$, $\exp(x+y) = e^{x+y} = e^x . e^y = \exp(x) . \exp(y)$

له بلي خوا د 0.4 مثال له مخې exp بایجکتیف دی.

قضیه2.1: $(G_1,\oplus)$ او $(G_2,\odot)$ دوه گروپه چې عینیت عناصریي $e_1 \in G_1$ او $e_2 \in G_2$ دي. که $\varphi: G_1 \to G_2$ یو G –Hom وي. بیا لاندي افادي صدق کوي:

(1) $\varphi(e_1) = e_2$

(2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$

ثبوت (1): مونږپوهیږوچې په یو گروپ کی $x \odot x = x$ یوازی د عینیت عنصر خاصیت دی.

$$\varphi(e_1) = \varphi(e_1 \oplus e_1) = \varphi(e_1) \odot \varphi(e_1) \quad [\ \text{G-Hom}\ \varphi\ ]$$

دانښيي چې $\varphi(e_1)$ عينيت عنصر د G_2 دی. اومونږپوهيږو چې يو ګروپ يوازی يوعينيت لري. پس بايد $\varphi(e_1) = e_2$ وي
اويا ثبوت په لاندي ډول :

$$e_2 \odot \varphi(e_1) = \varphi(e_1) = \varphi(e_1 \oplus e_1) = \varphi(e_1) \odot \varphi(e_1)$$
$$\Rightarrow \varphi(e_1) = e_2$$ [د 1.2 قضيي له مخې]

ثبوت (2): د له (1) مخې $e_2 = \varphi(e_1)$ دی.

$a \in G_1$

$$e_2 = \varphi(e_1) = \varphi(a \oplus a^{-1}) = \varphi(a) \odot \varphi(a^{-1})$$

له دي څخه نتيجه اخلو چې $\varphi(a^{-1})$ معکوس د $\varphi(a)$ دی .
پس $\varphi(a^{-1}) = (\varphi(a))^{-1}$

قضيه 2.2: Homomorphism composition (هومومورفيزم ترکيب)

$(G,\oplus)$ ، $(G_1,\odot)$ او $(G_2,\ominus)$ دری ګروپونه دي . که $\varphi: G \longrightarrow G_1$ او $\varphi_1: G_1 \longrightarrow G_2$ دوه G-Hom وي. بيا $\varphi_1 o \varphi: G \longrightarrow G_2$ هم G-Hom دی.
ثبوت: $a, b \in G$

$$\varphi_1 o \varphi(a \oplus b) = \varphi_1 o\big(\varphi(a) \odot \varphi(b)\big)$$ [ځکه φ يو G-Hom]
$$= \varphi_1 o \varphi(a) \ominus \varphi_1 o \varphi(b)$$ [φ_1 يو G-Hom]

په نتيجه کی $\varphi_1 o \varphi$ يو G-Hom دی

تعريف 2.3: $(G,\oplus)$ او $(G_1,\odot)$ دوه ګروپونه چې $e \in G$ او $e_1 \in G_1$ يي عينيت عناصراو $\varphi: G \longrightarrow G_1$ يو G-Hom دی.بيا دالاندي سيت ته د φ هسته (kernel) ويل کيږي اومونږ هغه په kerφ سره ښيو

$$\text{Ker}\,\varphi := \{a \in G \mid \varphi(a) = e_1\}$$

$$\text{Im}(\varphi) := \{\varphi(a) \mid a \in G\} \subseteq G_1$$

دلته $\text{Im}(\varphi)$ د φ Image (نقش يا تصوير) دی

قضيه 2.3: $(G,\oplus)$ او $(G_1,\odot)$ ګروپونه چې $e \in G$ او $e_1 \in G_1$ يي دعينيت عناصر او $\varphi: G \longrightarrow G_1$ يو G-Hom دی. بيا:

$$\varphi \; injective \;\Leftrightarrow Ker\varphi = \{e\}$$

ثبوت: "⇒" بايد ثبوت شی چې $Ker\varphi = \{e\}$ کيږي.

که $Ker\varphi \neq \{e\}$ وي پدی صورت :

$Ker\varphi \neq \{e\} \Rightarrow \exists a \in G;\ a \neq e \ \wedge\ \varphi(a) = e_1$

له بلي خوا د 2.1 قضیی په اساس $\varphi(e) = e_1$

$\varphi(a) = e_1 = \varphi(e)$
$\Rightarrow a = e \qquad [$ ځکه φ یو $\text{injective}]$
$\Rightarrow Ker\varphi = \{e\}$

ثبوت: " $\Leftarrow$ " د $a, b \in G$ لپاره مونږ فرض کوچې $\varphi(a) = \varphi(b)$ وي.

$$\varphi(a \oplus b^{-1}) = \varphi(a)\odot\varphi(b^{-1})$$
$$= \varphi(a)\odot(\varphi(b))^{-1} \quad [\text{د } 2.1 \text{ قضیی په اساس}]$$
$$= \varphi(b)\odot(\varphi(b))^{-1} = e_1 \quad [\text{د فرضیی په اساس}]$$

$\Rightarrow a \oplus b^{-1} \in Ker\varphi$
$\Rightarrow a \oplus b^{-1} = e \quad [$ ځکه $Ker\varphi = \{e\}]$
$\Rightarrow a \oplus b^{-1} \oplus b = e \oplus b = b \quad \Rightarrow a = b$
$\Rightarrow \varphi$ injective

مثال 2.1 : دالاندي تابع یوه G-Aut ده

$$\varphi: (\mathbb{C}, +) \longrightarrow (\mathbb{C}, +)$$
$$z = (x + iy) \mapsto \bar{z} = (x - iy)$$

حل:

φ G-Hom :

$z = x + iy\ , z_1 = x_1 + iy_1 \in \mathbb{C}$

$$\varphi(z + z_1) = \varphi(x + iy + x_1 + iy_1) = \varphi(x + x_1 + (y + y_1)i)$$
$$= (x + x_1 - (y + y_1)i = (x + x_1 - iy - iy_1)$$
$$= x - iy + x_1 - iy_1 = \bar{z} + \bar{z}_1 = \varphi(z) + \varphi(z_1)$$

φ injective :

$z = x + iy\ , z_1 = x_1 + iy_1 \in \mathbb{C}$

که چیری $\varphi(z) = \varphi(z_1)$ وی باید ثبوت شی چی $z = z_1$

$$\varphi(z) = \varphi(x + iy) = \varphi(z_1) = \varphi(x_1 + iy_1)$$

$\Rightarrow \bar{z} = x - iy = x_1 - iy_1 = \bar{z}_1 \Rightarrow x = x_1 \ \wedge\ -iy = -iy_1$

$\Rightarrow x = x_1 \ \wedge\ iy = iy_1 \Rightarrow z = x + iy = x_1 + iy_1 = z_1$

$\Rightarrow \varphi$ injective

: surjective φ

د $x + iy \in \mathbb{C}$ لپاره مونږ یو z_1 مساوی د x - iy مساوی د z_1 لپاره وضع کوو

$\varphi(z_1) = \varphi(x - iy) = x + iy = z$

څرنګه چې φ یو G-Hom او بیجکتیف دی. پس یو G-Aut دی

ker φ = {0} . ځکه φ یو injective او صفرعینیت عنصر د $(\mathbb{C}, +)$ دی

مثال 2.2 **:** دالاندي تابع پر $(A^{(2,2)}, \odot)$ ګروپ باندی تعریف شویده :

$$\varphi: (A^{(2,2)}, \odot) \longrightarrow (A^{(2,2)}, \odot)$$

$$a \longrightarrow a \odot a$$

G-Hom : باید وښودل شي چې د $\forall x, y \epsilon (A^{(2,2)})$ لپاره لاندي افاده صدق کوي :

$$\varphi(x \odot y) = \varphi(x) \odot \varphi(y)$$

مونږپوهیږوچې b_1 د $A^{(2,2)}$ عینیت عنصراو دهر $\forall x \epsilon (A^{(2,2)}$ لپاره:

$x \odot x = b_1$

$z := x \odot y \in (A^{(2,2)}$

$\varphi(x \odot y) = \varphi(z) = z \odot z = b_1$

$\varphi(x) = x \odot x = b_1 \wedge \varphi(y) = y \odot y = b_1$

$\Longrightarrow \varphi(x) \odot \varphi(y) = b_1 \odot b_1 = b_1$

$\Longrightarrow \varphi(x \odot y) = b_1 = \varphi(x) \odot \varphi(y) \Rightarrow \varphi$ G-Hom

څرنګه چې φ یو تابع له $(A^{(2,2)})$ څخه پر $(A^{(2,2)})$ ده . پس یو φ G-Endom دی .

:Injective $x, y \epsilon A^{(2,2)}$. که $\varphi(x) = \varphi(y)$ وي باید ثبوت شي چې y = x دی . یعني :

$x, y \epsilon (A^{(2,2)})$; $\varphi(x) = \varphi(y) \Rightarrow x = y$

$\varphi(b_3) = b_3 \odot b_3 = b_1 = b_2 \odot b_2 = \varphi(b_2)$

مګر $b_2 \neq b_3$ دی . پس φ یو injective نه دی .

:Surjective باید ثبوت شي چې د هر $y \epsilon A^{(2,2)}$ لپاره یو $x \epsilon A^{(2,2)}$ موجود وی چې $\varphi(x) = y$ شي . یعني :

$\forall y \in (A^{(2,2)}), \exists x \epsilon A^{(2,2)} ; \varphi(x) = y$

خرنګه چې $b_3 \in A^{(2,2)}$ لپاره هیڅ یو عنصر $x\epsilon\ (A^{(2,2)})$ وجود نه لري چې
$\varphi(x) = b_3$ شي. پس surjective نه دی اوپه نتیجه کی φ یو G-Autom
هم نه دی . اوس غواړو $\text{Ker}\ \varphi$ پیداکړو

$$\text{Ker}\ \varphi \coloneqq \left\{a \in A^{(2,2)} \,\middle|\, \varphi(a) = b_1\right\}$$

دجدول له مخی:

$$\forall\, a \in A^{(2,2)}\ ;\ \varphi(a) = a \odot a = b_1 \Rightarrow \text{Ker}\ \varphi = A^{(2,2)}$$

مثال 2.3: مونږپوهیږو چې G={1,-1} نظرضرب ته یو ګروپ دی. په 1.9 مثال کی مو ولیدل چې $(Q_8, .)$ هم یو ګروپ دی. φ په لاندي ډول تعریف شوي ده:

$$\varphi:\ (Q_6\,,*\,) \longrightarrow (G, .\,)$$

$$\varphi\ (e) = \varphi\ (a) = \varphi\ (b) = 1 \quad \wedge\ \varphi\ (c) = \varphi\ (d) = \varphi\ (f) = -1$$

په اسانی سره ښودلای شوچې φ یو G-Hom دی. د مثال په ډول

$$\varphi(d*f) = \varphi(b) = 1 = (-1).(-1) = \varphi(d).\,\varphi(f)$$

ker ϕ : خرنګه چې عینیت په G کی 1 (یو) دی. پس

$$\ker\varphi = \{x \in Q_6\ |\varphi(x) = 1\} = \{\, e,a,b\, \}$$

مثال 2.4 :

$$G \coloneqq \{A \in M(2x2, \mathbb{R}) \,|\, A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix}, xt\ \neq 0\}$$

(a) G نظرد ماتریکسو ضرب ته یو ګروپ دی

(b) دا لاندي تابع G-Hom ده

$$\varphi : (G, .) \ \longrightarrow (\mathbb{R}^*\,, .)$$

$$A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix} \longmapsto\ xt$$

ثبوت (a)

(G,.) الجبری جوړښت لري . ځکه:

$$A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix}, B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \text{G}$$

$$A.B = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix} . \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & xb+yc \\ 0 & tc \end{pmatrix}$$

له بلي خوا:

$$xt \neq 0 \ \wedge \ ac \neq 0 \ \Longrightarrow x \neq 0 , t \neq 0 , a \neq 0 , c \neq 0$$
$$\Longrightarrow \ xa.tc \neq 0 \quad \Longrightarrow A.B \in G$$

اویاپه بله طریقه

$$xt \neq 0 \ \wedge \ ac \neq 0$$
$$\Longrightarrow \ \det(A) \neq 0 \ \wedge \ \det(B) \neq 0$$
$$\Longrightarrow \ \det(A.B) = xa.tc = xt.ac \neq 0 \Longrightarrow A.B \in G$$

عینیت عنصر: د E_2 ماتریکس عینیت (identity) دی اوپه G کی شامل دی اتحادی خاصیت (associativity) هم صدق کوي

د معکوس (inverse) موجودیت :

$$A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix} \in G \ \Rightarrow \ x.t \neq 0 \ \Rightarrow \ x \neq 0 , t \neq 0$$

$$\left.\begin{pmatrix} x & y \\ 0 & t \end{pmatrix}\right| \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ . \frac{1}{x}$$

$$\left.\begin{pmatrix} 1 & \frac{y}{x} \\ 0 & t \end{pmatrix}\right| \begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 1 \end{pmatrix} \ . \frac{1}{t}$$

$$\left.\begin{pmatrix} 1 & \frac{y}{x} \\ 0 & 1 \end{pmatrix}\right| \begin{pmatrix} \frac{1}{x} & 0 \\ 0 & \frac{1}{t} \end{pmatrix} \ -\frac{y}{x} .$$

$$\left.\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right| \begin{pmatrix} \frac{1}{x} & \frac{-y}{xt} \\ 0 & \frac{1}{t} \end{pmatrix}$$

$$\Rightarrow \ A^{-1} = \begin{pmatrix} \frac{1}{x} & \frac{-y}{xt} \\ 0 & \frac{1}{t} \end{pmatrix}$$

په اسانی بنودلای شو چې $A^{-1} \in G$ او $A . A^{-1} = E_2$ کيږي

اویا د الجبرخطی له مخی :

$$x.t \neq 0 \Longrightarrow \det(A) \neq 0 \Longrightarrow A \text{ invertible}$$

ثبوت (b)

$A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix}, B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{G}$

$\varphi(\mathrm{A.B}) = \varphi\left(\begin{pmatrix} xa & xb+yc \\ 0 & tc \end{pmatrix}\right) = (\mathrm{xa})(\mathrm{tc}) = (\mathrm{xt}).(\mathrm{ac})$

$= \varphi(A).\varphi(B)$

ker φ : څرنګه چې عینیت په $(\mathbb{R}^*, .)$ کي 1 (یو) دی. پس :

$\ker\varphi = \{\mathrm{A} \in \mathrm{G} \mid \varphi(\mathrm{A}) = 1\} = \{A \in G \mid A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix}, xt = 1\}$

$= \{\mathrm{A} \in \mathrm{G} \mid \mathrm{A} = \begin{pmatrix} \mathrm{x} & \mathrm{y} \\ 0 & \mathrm{t} \end{pmatrix}, \mathrm{t} = \frac{1}{\mathrm{x}}\}$

تقسیم پرx اجازه لرو. څکه x خلاف د صفر دی . د مثال په ډول

$\begin{pmatrix} 2 & y \\ 0 & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} -2 & y \\ 0 & -\frac{1}{2} \end{pmatrix} \in \ker\varphi$

څرنګه چې $\ker\varphi \neq \{1\}$ دی ، پس د **2.3** قضیی له مخی φ اینجکتیف نه دی.

د مثال په ډول:

$A = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$

φ(A) = 2 = φ(B) دی، مګر A او B سره مساوی نه دي

مثال 2.5: $(V, \mathbb{R})$ او $(W, \mathbb{R})$ وکتوری فضاوی دي.

$\mathrm{L}: \mathrm{V} \longrightarrow \mathrm{W} \ \text{lin-Map} \implies \mathrm{L}: (\mathrm{V},+) \longrightarrow (\mathrm{W},+) \ \text{G-Hom}$

حل: وکتوری فضا د تعریف له مخی (V,+) او(W,+) تبدیلی ګروپونه دي

x,y∈V ⟹ L(x + y) = L(x) + L(y) [څکه L میپینګ خطی است]

⟹ L G-Hom

تمرین 2.1:

(a)

$\varphi : (\mathbb{C}, +) \longrightarrow$

$\mathrm{z} = \mathrm{a} + \mathrm{ib} \mapsto |z| = \sqrt{\mathrm{a}^2 + \mathrm{b}^2}$

ایا φ یو G-Hom دی

(b)

$\varphi : (\mathbb{C}^*,.) \longrightarrow (\mathbb{R}^*,.)$

$z = a + ib \mapsto \ |z| = \sqrt{a^2 + b^2}$

ثبوت کړی چې φ یو G-Hom دی او ker φ پیدا کړی

قضیه 2.4: $(G,\oplus)$ او $(G_1,\odot)$ گروپ دي چې عینیت عناصریي $e \in G$ او $e_1 \in G_1$ دي. که $\varphi: G \longrightarrow G_1$ یو G_Hom وي بیا:

(1) $(Ker\varphi,\oplus)$ هم گروپ دی .

(2) $(\varphi(G)\ ,\odot\ )$ هم گروپ دی

ثبوت(1):

$a,b \in Ker\varphi$

$\Rightarrow \varphi(a \oplus b) = \varphi(a)\odot\varphi(b)$

$= e_1\odot e_1$ [ځکه دي عناصر $Ker\varphi$ د b او a]

[ځکه a او b د $Ker\varphi$ عناصر دي]

$= e_1 \Rightarrow a \oplus b \in Ker\varphi$

ولیدل شوچې ($Ker\varphi$, $\oplus$) یوالجبري جوړښت (algeb-struct) لري.

اتحادی خاصیت: څرنگه چې $Ker\varphi \subseteq G$ او $\oplus$ پر $Ker\varphi$ بانه دي هم تطبیق کیږي. پس $Ker\varphi$ هم اتحادی خواص لري.

دعینیت موجودیت :

$e \in G \Longrightarrow \varphi(e) = e_1 \qquad \Longrightarrow e \in Ker\varphi$

د معکوس موجودیت :

$a \in Ker\varphi \subseteq G \Longrightarrow \varphi(a) = e_1$

$\Longrightarrow (\varphi(a))^{-1} = e_1$

$\Longrightarrow \varphi(a^{-1}) = e_1$ [نظر 2.1 قضیه]

$\Longrightarrow a^{-1} \in Ker\varphi$

ثبوت (2) : غواړوثبوت کړو چې ($\varphi(G)$, $\odot$) یوگروپ دی

$a_1,b_1 \in \varphi(\mathrm{G}) \Longrightarrow \exists a,b \in G; \varphi(a) = a_1 \wedge \varphi(b) = b_1$

$\Longrightarrow a_1\odot b_1 = \varphi(a \oplus b) = \varphi(a)\odot\varphi(b)$

$\Longrightarrow a_1\odot b_1 \in \varphi(\mathrm{G})$

ثبوت شوچې $(\varphi(G), \odot)$ یوالجبری ساختمان لري .

اتحادی خاصیت:

$a_1, b_1, c_1 \in \varphi(\mathrm{G})$

$\exists a, b, c \in G;\ \varphi(a) = a_1 \wedge \varphi(b) = b_1 \quad \wedge \varphi(c) = c_1$

$$a_1 \odot (b_1 \odot c_{1)} = \varphi(a) \odot \big(\varphi(b) \odot \varphi(c)\big)$$
$$= \big(\varphi(a) \odot \varphi(b)\big) \odot \varphi(c)$$
$$= (a_1 \odot b_1) \odot c_1$$

دعینیت موجودیت :

$\varphi(e) = e_1 \Rightarrow e_1 \in \varphi(\mathrm{G})$

د معکوس موجودیت:

$a_1 \in \varphi(\mathrm{G}) \Rightarrow \exists a \in G; \varphi(a) = a_1 \ \wedge \ \exists a^{-1} \in G; a \oplus a^{-1} = e$

$\Rightarrow \varphi(a) \odot \varphi(a^{-1}) = \varphi(\mathrm{a} \oplus a^{-1}) = \varphi(e) = e_1$

$\Rightarrow \mathrm{a}_1 . \varphi(a^{-1}) = \mathrm{e}_1$

په نتیجه کی $\varphi(a^{-1})$ معکوس د a_1 دی.

قضیه 2.5: $(G, \oplus)$ ، $(G_1, \odot)$ او $(G_2, \ominus)$ گروپونه دي . بیا :

(1) که $\varphi: G \longrightarrow G_1$ یو G-Isom وي. بیا د φ معکوس $\varphi^{-1}: G_1 \longrightarrow G$ هم G-Isom دی.

(2) که $\varphi: G \longrightarrow G_1$ او $\varphi_1: G_1 \longrightarrow G_2$ G_Isom وې. بیا د هغوی ترکیب $\varphi_1 o \varphi: G \longrightarrow G_2$ هم G-Isom دی.

ثبوت(1): مونږپوهیږوچې دیوی بایجکتیفی (Bijective) تابع معکوس هم بایجکتیف (Bijective) دی. پس کفایت کوي ثبوت شی چې φ^{-1} یو G-Hom دی.

$a_1, b_1 \in G_1$

$\Rightarrow \ \exists a, b \in G; \varphi(a) = a_1 \wedge \varphi(b) = b_1 \quad [\ \varphi$ surjective $]$

$\Rightarrow \varphi(\mathrm{a} \oplus \mathrm{b}) = \varphi(a) \odot \varphi(b) = a_1 \odot b_1 \quad [\ \varphi \quad$ G-Hom $]$

$\Rightarrow \varphi^{-1}(a_1 \odot b_1) = \varphi^{-1}\Big(\varphi(\mathrm{a} \oplus \mathrm{b})\Big) = \varphi^{-1} o \varphi(a \oplus b)$

$$= \mathrm{id}(a \oplus b) = a \oplus b$$

څرنګه چې :

$\varphi(a) = a_1 \ \wedge \ \varphi(b) = b_1$

$\Rightarrow \varphi^{-1}(a_1) = a \ \wedge \ \varphi^{-1}(b_1) = b$

پس:

$$\varphi^{-1}(a_1 \odot b_1) = \varphi^{-1}(a_1) \oplus \varphi^{-1}(b_1)$$

ثبوت شوچې φ^{-1} یو G-Isom دی.

ثبوت(2): د 2.2 قضیې په اساس کفایت کوی ثبوت شي چې $\varphi_1 o \varphi$ یو بایجکتیف (bijective) دی.

: Injective

$a, b \in G, \varphi_1 o \varphi(a) = \varphi_1 o \varphi(b)$

$\Rightarrow \varphi(a) = \varphi(b)$ [injective φ_1 ځکه]

$\Rightarrow a = b$ [injective φ ځکه]

ثبوت شو چې $\varphi_1 o \varphi$ یو injective دی .

: Surjective

$g_2 \in G_2 \Rightarrow \exists g_1 \in G_1, \varphi_1(g_1) = g_2 \ \wedge \ \exists g \in G; \varphi(g) = g_1$

$\Rightarrow \ \varphi_1(\varphi(g)) = \varphi_1(g_1) = g_2$

$\Rightarrow \ \varphi_1 o \varphi$ surjective

تمرین 2.2: کوم یودلاندي توابعو څخه surjective , injective او G-Hom دي او کومي نه دي

(a) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
$z \longmapsto 2z$

(b) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
$z \longmapsto z+1$

(c) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, .)$
$x \longmapsto x^2+1$

(d) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, .)$

$x \mapsto \frac{2}{3} \cdot (x-1)$

(e) $f : (\mathbb{R}^*, .) \longrightarrow (\mathbb{R}^*, .)$
$x \mapsto x^2$

تمرین 2.3 : (G,.) یک گروپ او e دهغه عینیت عنصردی. $a \in G$

$L_a : G \longrightarrow G$
$x \mapsto a.x.a^{-1}$

ثبوت کړی چې L_a یو G-Aut دی او $\ker(L_a)$ پیداکړی .

تمرین 2. 4 : $(G, \odot)$ یو گروپ او e د هغه عینیت عنصر دی.

$f : G \longrightarrow G$
$a \mapsto a \odot a$

که f یو G-Hom وی. ثبوت کړی چې G یوتبدیلی گروپ (commutative) دی

تمرین 2.5 : په 1.11 مثال کی مو ولیدل چې $(Q_4, .)$ یــو گروپ دی

$f : (A^{(2,2)}, \odot) \longrightarrow (Q_4, .)$
$b_1 \mapsto E \ , \ b_2 \mapsto A$
$b_3 \mapsto B \ , \ b_4 \mapsto C$

ایا پورتنی تابع یو G-Hom ده

تمرین 2.6 : $\varphi : (G,.) \longrightarrow (G_1,*)$ یو G – isom دی. بیا:

(a) G Commutative $\Leftrightarrow$ G_1 Commutative

(b) $|G| = |G_1|$

دريم فصل

فرعی گروپ (Subgroup)

تعریف 3.1: $(G,\oplus)$ یو گروپ دی او $H \subseteq G$.

H ته فرعی گروپ (Subgroup) واي, که چیري H خپله نظر $\oplus$ دوه گوني رابطې ته گروپي جوړښت ولري. یعني $(H , \oplus)$ یو گروپ وې.

مثال:

(a) G او {e} دوړه فرعی گروپونه د G گروپ دي ، چې e عینت عنصر دی

(b) $\mathbb{Z}$ یو فرعی گروپ د $\mathbb{Q}$ نظرجمع "+" ته دی.

(c) $\mathbb{Q}$ یو فرعی گروپ د $\mathbb{R}$ نظرجمع "+" ته دی.

(d) $\mathbb{Q}^*$ یو فرعی گروپ د $\mathbb{R}^*$ او $\mathbb{R}^*$ یو فرعی گروپ د $\mathbb{C}^*$ نظرضرب "." ته دي .

(e) $H=\{a_0,a_2\}$ یو فرعی گروپ د $A^{(4)}$ دی .

قضیه3.1: $(G,\oplus)$ یو گروپ چی e یي عینیت عنصر دی او $H \subseteq G$. بیا:

$$(H,\oplus) \text{ یوفرعې گروپ } \Leftrightarrow \begin{cases} (1)\ a,b \in H, a\oplus b \in H \\ (2)\ e\in H \\ (3)\ a \in H \Rightarrow a^{-1} \in H \end{cases}$$

ثبوت " $\Leftarrow$ ": دا چې H یو فرعی گروپ په G کې دی ، پس (1) صدق کوي.

(2) **ثبوت:** که $\tilde{e}$ عینیت عنصر د H وي، پس:

$$\tilde{e} \in H \Rightarrow \tilde{e} \in G \ \wedge \ \tilde{e}\oplus\tilde{e} = \tilde{e}$$

دا هغه وخت امکان لري چې $\tilde{e}$ عینیت عنصر د G وي. یعني $\tilde{e} = e$. پس $e\in H$ دی.

(3) **ثبوت :**

$e,a \in H \Rightarrow \exists b \in H; a\oplus b = e$ [1.2 قضیي له مخې]

څرنګه چې G یو گروپ دی. پس b باید معکوس د a (یعنې $b = a^{-1}$) وی.

په نتیجه کې: $b = a^{-1} \in H$

ثبوت " $\Rightarrow$ ": نظر (2) ته د H سیت خالی ندی او نظر (1) ته د $\oplus$ دوه گوني رابطه هم صدق کوي . نظر (2) او (3) ته د H سیت عینیت اودهرعنصرلپاره معکوس لري. پس نظر $\oplus$ ته یو فرعی گروپ دی.

قضیه 3.2: $(G,\oplus)$ یو گروپ ، $e \in G$ عینیت عنصر او $H \subseteq G$. بیا:

$$\left.\begin{array}{l}(1)\ H \neq \emptyset \\ (2)\ \forall a,b \in H, a\oplus b^{-1} \in H\end{array}\right\} \Leftrightarrow \text{یوفرعي گروپ } (H,\oplus)$$

ثبوت" $\Leftarrow$ " : واضح ده چې هر فرعی گروپ دا خواص لري یعنې:

$e \in H \ \Rightarrow \ H \neq \emptyset$

$\forall a,b \in H,\ \exists\, b^{-1} \in H \ \wedge\ a\oplus b^{-1} \in H$

ثبوت" $\Rightarrow$ " : د 3.1 قضیي له مخې باید ثبوت شي چې H د هغي قضیي (1) , (2) او (3) خواصه لري .

$\text{H} \neq \emptyset \Rightarrow \exists\, a \in H \Rightarrow e = a\oplus a^{-1} \in H \Rightarrow (2)$

$a,e \in H \Rightarrow e\oplus a^{-1} \in H \Rightarrow e\oplus a^{-1} = a^{-1} \in H \Rightarrow (3)$

$a,b \in H \Rightarrow a\oplus b^{-1} \in H$ [نظر (2) ته]

پورته وښودل شول چې (3) د 3.1 قضیي صدق کوي. پس $b^{-1} \in H$ دی .

$\Rightarrow a\oplus(b^{-1})^{-1} \in H$ [نظر (2) ته]

$\Rightarrow \quad a\oplus(b^{-1})^{-1} = a\oplus b \in H \Rightarrow (1)$

مثال : په ($A^{(2,2)}$, ⊙) گروپ کې علاوه پر $A^{(2,2)}$ او {b$_1$} د H:={b$_1$, b_2} سیت هم یو فرعی گروپ په $A^{(2,2)}$ کې دی. ځکه عینیت عنصریی b$_1$ په H کې شامل او b$_2$ ⊙ b$_2$ = b$_1$ کیږي .

مثال : د $(D_4,.)$ په گروپ کې علاوه پر D_4 او {e} د {e,b} ، H:={e,a,b,c} سیتونه هم فرعی گروپونه په D_4 دي.

که *H:={e,a,b,c}* یو فرعی گروپ د D_4 وي ، باید 3.1 قضیي (1) , (2) او (3) ولري

$e \in H \Longrightarrow (2)$

د D_4 جدول له مخې :

$a.a = b \in H \ , a.b = c \in H \ , a.c = e \in H \ , \ b = e \in H,$

$c.c = b \in H \quad \Longrightarrow (1)$

ځرنګه چې a معکوس د c او د c معکوس a دی اود b معکوس خپله b دی.
پس (3) هم صدق کوي. په نتیجه کې H={e,a,b,c} یوفرعی ګروپ د D_4 دی.
تمرین : کوم یو د لاندي سیتو څخه فرعی ګروپ په D_4 کي دي
$H_1 = \{b,f,h\}$, $H_2 = \{e ,b,d,g \}$, $H_3 = \{e , f \}$, $H_4 = \{e,b,c\}$,
$H_5= \{e,a\}$
مثال : په $(Q_8 , .)$ ګروپ کې علاوه پر Q_8 او $\{e\}$ د H:= {e,a,d,f} سیت هم دهغه فرعی ګروپ دی. ځکه (1) او (2) د 3.1 قضیه صدق کوي. اوس باید وښیو چې معکوس د $\forall x \in H$ هم په H کې شامل دی

$$d.f = e \implies d^{-1} = f \quad \wedge \quad f^{-1} = d \implies d^{-1}, f^{-1} \in H$$
$$a.a = e \implies a = a^{-1} \implies a^{-1} \in H$$

په نتیجه کې { H={e,a,d,f یو فرعی ګروپ په Q_8 کې دی .
مثال 3.A: د 1.9 په مثال کی مو ولیدل چې (Q , .) یو ګروپ دی.
(1) د $Q_1 := \{E,-E,I,-I\}$ سیت یو فرعی ګروپ په (Q , .) کي دی. ځکه مونږپوهیږو چې E عینیت عنصر د Q او $E \in Q_1$ دی. د کیلي جدول له مخې:
$(-E).(-E) = E$, $(-E).I = -I$, $(-E).(-I) = I$,

$I.I = -E$, $I.(-I)=E$, $(-I).(-I) = -E$

د -E معکوس خپله –E ، د I معکوس –I او –I معکوس I دی. پس لیکلی شو:

$$\forall A,B \in Q_1 \implies A.B \in Q_1 \quad \wedge \quad A^{-1} \in Q_1$$

په نتیجه کی د **3.1** قضی له مخې Q_1 یوفرعي ګروپ د Q دی.
(2) په 1.6 مثال کی مو ولیدل چې $(GL(2, \mathbb{R}),.)$ یوګروپ دی او عینیت عنصریی واحد متریکس $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ دی.

$N:= \{ A \in (GL(2, \mathbb{R}),.) \mid \det A = 1 \}$
$H:= \{ A \in (GL(2, \mathbb{R}),.) \mid$ A diagonal (قطری) $\}$
$M:= \{ A \in GL(2, \mathbb{R}) \mid A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \}$

N ، M او H فرعی ګروپونه د $GL(2, \mathbb{R})$ دي
حل: حل لپاره د 3.1 قضیی څخه استفاده کوو.
$A, B \in N \implies \det A = \det B = 1$
$\det(A.B) = \det A . \det(B) = 1.1 = 1 \implies A.B \in N$
$\det(E_2) = 1 \implies E_2 \in N$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N \Rightarrow \det A = ad - bc = 1$

$A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$\det(A^{-1}) = ad - bc = 1 \Rightarrow A^{-1} \in N$

په نتیجه کی N فرعی گروپ د (GL(2, ℝ دی.

$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \in H$

$A \,.\, B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \in H \;,\; E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$

$\det A = ab \neq 0$ [$A \in (GL(2, \mathbb{R}), .)$ ځکه]

$\Rightarrow a \neq 0 \;\wedge\; b \neq 0$

$A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} = \frac{1}{ab} \cdot \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix} \in H$

ثبوت شو چې H هم يو فرعی گروپ د (GL(2, ℝ دی.

$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$

$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in M$

$A.B = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \in M$

$\det A = 1 \neq 0$

$A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = 1 \,.\, \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \in M$

ثبوت شو چې M هم يو فرعی گروپ د (GL(2, ℝ دی.

تمرين 3.1:

(a) کوم یودلاندي سیټوڅخه فرعی گروپونه په (D_4 ,.) گروپ کې دي

$H_1 = \{b,f,h\}$, $H_2 = \{e ,a,g,h \}$, $H_3 = \{e , f \}$,

$H_4 = \{e,b,c\}$, $H_5 = \{e,a\}$

(b) کوم یودلاندي سیټوڅخه فرعی گروپونه په (Q_8 ,.) گروپ کې دي

$H_1 = \{c,f,h\}$, $H_2 = \{e ,a,g,h \}$, $H_3 = \{e , f \}$,

$H_4 = \{e,b,c\}$, $H_5 = \{e,a\}$

(c) کوم یودلاندي سیتوڅخه فرعی ګروپونه په (.,Q) کې دي

$H_1 = \{E,-E\}$, $H_2 = \{E ,I,K \}$, $H_3 = \{-E , -K\}$, $H_4 = \{E,-E,I,-I\}$,
$H_5 = \{E,K\}$

مثال:

(a) $H := \{a \in \mathbb{Z} \mid -6 \le a \le 6\}$

H فرعی ګروپ د $(\mathbb{Z},+)$ کیدای نه شي . ځکه : $5 + 6 = 11 \notin H$

(b) $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x > 0\}$

$\mathbb{R}_+$ فرعی ګروپ (subgroup) د $(\mathbb{R},+)$ نه دی . ځکه صفر "0" چې نظر جمع "+„ ته عینیت عنصر د $\mathbb{R}$ دی.مګرصفر په $\mathbb{R}_+$ کې شامل نه دی.

تمرين 3.2 :

(a)

$M := \{A \in M(2x2,\mathbb{R})\}$

$N := \{A \in M(2x2,\mathbb{R}) \mid A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\}$

په 1.1 مثال کی مووليدل چې (M,+) ګروپی جوړښت لری.ثبوت کړي چې N دهغه يو فرعی ګروپ دی.

(b) ثبوت کړی چې $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x > 0\}$ يو فرعی ګروپ په $(\mathbb{R}^*,.)$ کې دی.

قضيه 3.3: $(G,\oplus)$ ، $(G_1,\odot)$ ګروپونه چې $e \in G$ او $e_1 \in G_1$ د هغوی عینیت عناصر دي. که $H \subseteq G$ او $H_1 \subseteq G_1$ فرعی ګروپونه او $\varphi: G \longrightarrow G_1$ يو G-Hom وي. بیاً:

(a) $\boldsymbol{\varphi}^{-1}(H_1)$ يو فرعی ګروپ د G دی.

(b) $\varphi(H)$ يو فرعی ګروپ د G_1 دی.

(a)ثبوت :

$\varphi(e) = e_1$ [د 2.1 قضيي له مخې]

$\Rightarrow \varphi^{-1}(e_1) = e \Rightarrow e \in \varphi^{-1}(H_1)$

$\Rightarrow \varphi^{-1}(H_1) \neq \phi$

د 3.2 قضيي له مخې کفايت کوې ثبوت کړو چې دهر $a, b \in \varphi^{-1}(H_1)$ لپاره بايد همدارنګه $a \oplus b^{-1} \in \varphi^{-1}(H_1)$ صدق وکړي .

$a, b \in \varphi^{-1}(H_1) \Rightarrow \varphi(a), \varphi(b) \in H_1$

$$\Rightarrow \varphi(a \oplus b^{-1}) = \varphi(a) \odot \varphi(b^{-1}) = \varphi(a) \odot \varphi(b)^{-1} \in H_1$$

$$\Rightarrow a \oplus b^{-1} \in \overset{-1}{\varphi}(H_1)$$

پس $\overset{-1}{\varphi}(H_1)$ یوفرعي ګروپ د G دی .

(b) ثبوت:

$\varphi(e) = e_1 \in \varphi(H) \Rightarrow \varphi(H) \neq \phi$

$a_1, b_1 \in \varphi(H) \Rightarrow \exists\, a, b \in H;\ \varphi(a) = a_1 \ \wedge\ \varphi(b) = b_1$

$$\Rightarrow \varphi(a \oplus b^{-1}) = \varphi(a) \odot \varphi(b^{-1})$$

$$= \varphi(a) \odot \varphi(b)^{-1} \ = a_1 \odot {b_1}^{-1} \in \varphi(H)$$

په نتیجه کې $\varphi(H)$ یو فرعی ګروپ د G دی.

مثال: پر $A^{(4)}$ ⊆ H={a_0,a_2} فرعی ګروپ او $A^{(2)}$ ګروپ باندې لاندې تابع تعریف شویده

$$f : H \longrightarrow A^{(2)}$$

$$x \mapsto \begin{cases} e & if \quad x = a_0 \\ a & if \quad x = a_2 \end{cases}$$

f یو G-Isom دی. ځکه:

$$f(a_0 \oplus a_0) = f(a_0) = e = e \odot e = f(a_0) \odot f(a_0)$$

$$f(a_0 \oplus a_2) = f(a_2) = a = e \odot a = f(a_0) \odot f(a_2)$$

$$f(a_2 \oplus a_2) = f(a_0) = e = a \odot a = f(a_2) \odot f(a_2)$$

همدارنګه لیدل کیږي چې f یو بایجکتیف bijective دی. په نتیجه کې f یو G-Isom دی.

تعریف 3.2 : یو (G,.) ګروپ چې د ټولوعناصرو مولد (generator) یي یوازې د هغه یوعنصروي، د دورانی ګروپ (cyclic group) په نوم یادیږي.
یعني که یو a∈ G موجود وي چې د G ټول عناصرد a څخه لاس ته راشي .
یعني:

$$\forall\, b \in G,\ \exists i \in \mathbb{N};\ a.a......a\ (\text{i - دفعه}) = a^i = b$$

که a مولد (generator) د G ګروپ وي، مونږ هغه بیا په $\langle a \rangle = G$ سره ښیو.

مثال: ځرنګه چې $\mathbb{Z} = \{n.1 | n \in \mathbb{Z}\}$ دی . پس $(\mathbb{Z}, +)$ دورانی ګروپ دی.
یعنې $\langle 1 \rangle = (\mathbb{Z}, +)$
د مثال په ډول

$5.1=1+1+1+1+1 = 5$, $-5 = -5.1 = -(1+1+1+1+1)$

همدارنګه $\langle -1 \rangle = (\mathbb{Z}, +)$. ځکه: $\mathbb{Z} = \{n.(-1) | n \in \mathbb{Z}\}$
د مثال په ډول

$3 = -(3.(-1) = -(-1-1-1)$, $-3 = 3.(-1) = (-1-1-1)$

مثال: $(A^{(4)}, \oplus)$ یو دورانی ګروپ دی. ځکه:

$\langle a_1 \rangle = (A^{(4)}, \oplus)$

$a_1^1 = a_1$, $a_1^2 = a_1 \oplus a_1 = a_2$,

$a_1^3 = a_1 \oplus a_1 \oplus a_1 = a_2 \oplus a_1 = a_3$,

$a_1^4 = a_1 \oplus a_1 \oplus a_1 \oplus a_1 = a_3 \oplus a_1 = a_0$

همدارنګه $< a_3 >= (A^4, \oplus)$ دی
$A^{(2)}$ هم یو دورانی ګروپ (cyclic group) دی.
مګر $A^{(2,2)}$ یو دورانی ګروپ نه دی، ځکه:

$\forall\, b \in A^{(2,2)}\, ;\ b^2 = b_1 \Rightarrow < b > = \{b, b_1\}$

یعنې هر b عنصر فقط د $\{b, b_1\}$ مولد کیدای شي. د مثال په ډول
$< b_2 >= \{b_2, b_1\}$
پس په $A^{(2,2)}$ کې هیڅ عنصروجود نه لري چې مولد (generator) د $A^{(2,2)}$ ګروپ وي.

نوټ : کیدای شي دوه عنصره مولد د یو ګروپ وي . د مثال په ډول د $A^{(2,2)}$ په ګروپ کې $<b_2, b_3 > = A^{(2,2)}$

$b_1 = b_2 \odot b_2 \ \wedge\ b_4 = b_2 \odot b_3$

همدارنګه $<b_3, b_4 >$ او $<b_2, b_4 >$ مولد د $A^{(2,2)}$ دي .

نوټ: مونږ کولای شو یو معین دورانی ګروپ (G,.) چې $G = <a>$ او e د هغه عینیت عنصردی په لاندې شکل ولیکو:

$G = \{ a, a^2, a^3, \ldots\ldots, a^n = e \}$

مثال: مونږ یو معین دورانی ګروپ (G,.) چې $G = <a>$ او e د هغه عینیت عصنردی په لاندې شکل لرو:

$G = \{ a, a^2, a^3, a^4, a^5, a^6 = e \}$

$H = \{a^2,a^4,a^6= e\}$ د G یو فرعی گروپ دی. ځکه:

$a^2. a^2 = a^4$, $a^2. a^4 = a^6 = e$,
$a^4. a^4 = a^8 = a^2. a^6 = a^2. e = a^2$

تمرین 3.3:

(a) دپورتني مثال G نورمولد عناصراو فرعی گروپونه پیدا کړئ
(b)

$H:=\{e,a,b,c\}$, $W:=\{e,b,f,h\} \subseteq D_4$

مونږ پوهیږو چې H او W فرعي گروپونه د D_4 دي. معلوم کړئ چې کوم یو یی دوراني نه دی.

تمرین 3.4:

(1) مونږ یو معین دورانی گروپ (G,.) چې G = <a> او e د هغه عینیت عنصردی په لاندې شکل لرو. فرعی گروپونه **(subgroup)** یي پیدا کړئ .

(a) $G = \{ a, a^2,a^3,....,a^9,a^{10}, a^{11} = e \}$

(b) $G = \{ a, a^2,a^3,....,a^{14},a^{15}, a^{16} = e \}$

(2) $H := \{ 2^n \mid n\epsilon\mathbb{Z} \}$

ثبوت کړئ چې H یو دورانی فرعی گروپ د $(\mathbb{Q}^*,.)$ دی

(3) هر معین دورانی گروپ (cyclic group) تبدیلی (commutative) دی

تعریف 3.3: $X \neq \emptyset$ یو سیت دی. $f: X \to X$ تابع ته پرموتیشن (Permutation) ویل کیږی ، که چیري f یو bijective وي . مونږ پرX ټول پرموتیشونه په S(X) سره ښیو. یعني:

$S(X) := \{f: X \longrightarrow X \mid f \quad bijective \}$

مثال : پر X = {1,2} باندې یوازې دوه لاندي پرموتیشنه موجود دي :

$$f_0: X \longrightarrow X \qquad f_1: X \longrightarrow X$$
$$1 \longmapsto 1 \qquad 1 \longmapsto 2$$
$$2 \longmapsto 2 \qquad 2 \longmapsto 1$$

د پرموتیشن (Permutation) شمیر پریو سیت باندی تابع د هغه عناصرودی. د مثال په ډول د X={a,b,c} پرموتیشن شمیرشپږدی. په عمومي صورت که X د عناصرو شمیرn وې ، بیا دهغه د پرموتیشن شمیر $n!$ (factorial) دی. یعني

$|X| = n \Rightarrow |S(X)| = n! \qquad (n! = 1.2.3 \dots . n)$

قضیه 3.4: که $X \neq \emptyset$ یو ست وي ، بیا S(x) نظر تابع ترکیب "map-composition" ته گروپ دی .

ثبوت:

دوه گوني رابطه (binary operation) :

باید ثبوت شي چې دا لاندي رابطه پر S(X) قابل د تطبیق ده.

$$\circ: S(X) \times S(X) \longrightarrow S(X)$$

$$(f,g) \longmapsto f\circ g$$

دا واضح ده. ځکه که دوه تابع بایجکتیف وې ، بیا د هغوي ترکیب هم بایجکتیف دی.

عینیت عنصر (identity) : د id تابع یی عینیت عنصر دی. ځکه:

$$(id \circ f)(x) = id \circ \big(f(x)\big) = f(x) \Rightarrow id \circ f = f$$

اتحادی خاصیت (associative): دا هم تابع د ترکیب له مخی واضح دی.

معکوس عنصر (inverse element):

$$f \in S(X) \Rightarrow f \ \ bijective$$

$$\Rightarrow f^{-1} \ bijective \quad \Rightarrow f^{-1} \in S(X)$$

$$(f^{-1} \circ f)(x) = x = id(x) \Rightarrow f^{-1} \circ f = id$$

S(X) د permutation Group په نوم یادیږي

نوټ 3.1 :

(a) د X = {1,2,3,...,n} لپاره مونږ $f \in S(X)$ په لاندي شکل لیکو:

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

(b) S(X) گروپ د $|X| > 2$ لپاره تبادلوی نه دی. د مثال په ډول X={1,2,3}

$$f_1 := \begin{pmatrix} 1 & 2 & 3 \\ f_1(1) & f_1(2) & f_1(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$f_2 := \begin{pmatrix} 1 & 2 & 3 \\ f_1(1) & f_1(2) & f_1(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$f_1 \circ f_2(1) = f_1(2) = 3 \quad , f_1 \circ f_2(2) = f_1(1) = 2$$
$$f_1 \circ f_2(3) = f_1(3) = 1$$

$$f_1 o f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_2of_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

لیدل کیږي چې $f_2of_1 \neq f_1of_2$ دی.

نوټ : که X={1 ,2,3,………n} وي ، بیا د S(X) گروپ په S_n ښیو. S_n ته n درجه (degree) یي (symmetric group) ویل کیږي .

تعریف 3.4 : $a,b\in \mathbb{Z}$.مونږ وایو چې b بر a قابل د تقسیم یا دویش وړ (a divided b) دی، که چیري یو عدد $c\in \mathbb{Z}$ موجود وي چې b = a.c شي او دا په a|b سره ښودل کیږي .

قضیه 3.5 : (division algorithm) $a,b\in \mathbb{Z}$ او $b \neq 0$, بیا فقط یوازي یو $r \in \mathbb{Z}$ او یو $q\in \mathbb{Z}$ دلاندي خواصوسره موجود دی:

$$a= q.b +r \qquad 0 \leq r < |b|$$

q د حاصل تقسیم (the quotient) او r د باقیمانده (the remainder) په نومو یادیږي .

ثبوت : د ثبوت لپاره مونږ $H:=\{ a - bq \mid q \in \mathbb{Z} ; a - bq \geq 0\}$ په پام کې نیسواوغواړو ثبوت کړو:

(a) $H \neq \emptyset$

ثبوت: د b لپاره دادوه لاندي حالتونه امکان لري .

لمړی حالت b > 0 : په دې حالت $q \leq \frac{a}{b}$ غوره کوو، بیا:

$$q \leq \frac{a}{b} \quad \Rightarrow \quad q.b \leq a \Rightarrow a - q.b \geq 0$$

دویم حالت b < 0 : په دې حالت $q \geq \frac{a}{b}$ غوره کوو، بیا:

$$q \geq \frac{a}{b} \quad \Rightarrow \quad q.b \leq a \Rightarrow a - q.b \geq 0$$

ولیدل شول چې په دوړو حالتو کې یو عدد q پیدا شو چې $a-q.b \in H$ کیږي پس $H \neq \emptyset$ دی. مونږ ترټولوکوچنی عنصرپه H کې په r سره ښیو.

$$r\in H \Rightarrow \exists q\in \mathbb{Z} ; r = a - b.q \wedge r \geq 0 \Rightarrow a = b.q+r$$

(b) $r<|b|$:

ثبوت: که $r < |b|$ نه وې ، پس باید $r \geq |b|$ وې . په دې صورت بیا $r \geq b$ کیږي . ځرنگه چه $b \neq 0$ دی پس باید $b >0$ اویا $b < 0$ وې .

: b > 0

$$b > 0 \quad \wedge \quad r \geq b \quad \Rightarrow \quad r - b \geq 0 \quad \wedge \quad r - b \leq r$$

$a = b.q + r \Rightarrow a - bq = r \Rightarrow a - bq - b = r - b$
$\Rightarrow a - b(q + 1) = r - b \geq 0$
$\Rightarrow r - b \in H$

$: \ b < 0$

$b < 0 \quad \wedge \ r \geq b \Rightarrow r + b \geq 0 \ \wedge \ r + b \leq r$
$a = b.q + r \Rightarrow a - bq = r \Rightarrow a - bq + b = r + b$
$\Rightarrow a - b(q - 1) = r + b \geq 0$
$\Rightarrow r + b \in H$

په دواړو حالتو کې ولیدل شو چې تر r کوچني اعداد $r - b$ او $r + b$ موجود دي. مګردا دهغه سره تضاد دی چې r ترټولوکوچنی عنصر په H کې انتخاب شوی وه . پس لهذا $r < |b|$ دی

اوس باید ثبوت شي چې فقط یوازې یو q اویو r د هغو خواصوسره موجود دی . که چیري q_1 او r_1 هم دا خواص ولري .یعنې

$q.b + r = a = q_1.b + r_1 \Rightarrow q.b - q_1.b = r - r_1$
$\Rightarrow b.(q - q_1) = r - r_1$
$\Rightarrow |b|\,|q - q_1| = |r - r_1|$

که $q = q_1$ نه وي، بیا:

$q \neq q_1 \Rightarrow |q - q_1| \geq 1 \Rightarrow |r_1 - r| \geq |b|$

دا بیا دهغه سره په تضاد کې ده چې $r_1, r < |b|$ انتخاب شوي وه. پس باید $q = q_1$ او $r = r_1$ وي .

مثال:

$a = 55 , b = 24 \Rightarrow 55 = 2.24 + 7$

دلته $q = 2 , r = 7$

$a = -55 , b = 24 \Rightarrow -55 = (-3).24 + 17$

دلته $q = -3 , r = 17$

$a = -55 , b = -24 \Rightarrow -55 = 3.(-24) + 17$

دلته $q = 3 , r = 17$

لیما 3.2 :

(a) د $\forall m \epsilon \mathbb{N}$ لپاره د $m\mathbb{Z} := \{mz \mid z \epsilon \mathbb{Z}\}$ سیټ د $(\mathbb{Z}, +)$ یو فرعي ګروپ دی .

(b) د فرعی ګروپو تقاطع بیاهم یو فرعی ګروپ دی.

(a) **ثبوت :** د 3.2 قضیې له مخې کفایت کوې چې ثبوت شې:

$(1)\ m\mathbb{Z} \neq \emptyset$
$(2)\ \forall\, a, b \epsilon m\mathbb{Z} ,\ a - b \epsilon m\mathbb{Z}$

لمړی حالت : m=0

پدي صورت $m\mathbb{Z} = \{0\}$ کیږي او $\{0\}$ یو فرعي ګروپ د $(\mathbb{Z}, +)$ دی.

دویم حالت : $m \neq 0$

$$0\epsilon\mathbb{Z} \Rightarrow m.0 = 0 \epsilon m\mathbb{Z} \Rightarrow m\mathbb{Z} \neq \emptyset \Rightarrow (1)$$

$$a,b\epsilon m\mathbb{Z} \Rightarrow \exists a_1, b_1 \epsilon\mathbb{Z}; a = ma_1 \wedge b = mb_1$$

$$\Rightarrow a - b = ma_1 - mb_1 = m(a_1 - b_1)$$

$$\Rightarrow a - b \epsilon m\mathbb{Z} \quad [a_1 - b_1 \epsilon \mathbb{Z} \text{ ځکه}] \Rightarrow (2)$$

بل ډول ثبوت:

د 2.1 نوټ په اساس دا لاندي تابع یو G-Hom ده

$$f: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$$
$$z \longmapsto mz$$

د 3.3 قضی له مخې $f(\mathbb{Z}) = m\mathbb{Z}$ یوفرعي ګروب د $(\mathbb{Z}, +)$ دی.

(b) ثبوت : که مونږ یو ګروپ $(G, .)$ د e عینیت عنصرسره ولرو او H_i $(i\epsilon I)$ یی فرعی ګروپونه وي. $I := \{1,2, \ldots, n\}$

دهغوی تقاطع په H بنیو. یعني

$$H := \cap_{i\epsilon I} H_i$$

اوس غواړو ثبوت کړوچې H یو فرعی ګروپ په G کې دی.

$$e\epsilon H_i \quad (\forall i \epsilon I) \Rightarrow e \epsilon H$$

$$a,b \epsilon H \Rightarrow a,b \epsilon H_i \quad (\forall i \epsilon I)$$

$$\Rightarrow a.b \epsilon H_i \quad (\forall i \epsilon I) \quad [\text{ځکه } H_i \text{ فرعی ګروپ}]$$

$$\Rightarrow a.b \epsilon H$$

$$a \epsilon H \Rightarrow a \epsilon H_i \quad (\forall i \epsilon I) \Rightarrow a^{-1} \epsilon H_i \quad (\forall i \epsilon I)$$

$$\Rightarrow a^{-1} \epsilon H$$

په نتیجه کې H د 3.1 قضیې له مخې یو فرعی ګروپ په G کې دی.

مثال: د **3.2** لیما له مخې پوهیږو چې $5\mathbb{Z} = \{5z \mid z\epsilon 5\mathbb{Z}\}$ یو فرعی ګروپ په $(\mathbb{Z}, +)$ کې دی. اوس غواړو دا د 2.3 قضیی له مخی ثبوت کړو

$$5.1 \epsilon 5\mathbb{Z} \Rightarrow 5\mathbb{Z} \neq \emptyset$$

$$a,b\epsilon 5\mathbb{Z} \Rightarrow \exists a_1, b_1 \epsilon\mathbb{Z}; a = 5a_1 \wedge b = 5b_1$$

$\Rightarrow a-b = 5a_1 - 5b_1 = 5(a_1 - b_1)$
$\Rightarrow a-b \ \epsilon\ 5\mathbb{Z}$ [ځکه $a_1 - b_1 \epsilon\ \mathbb{Z}$ دی]
په نتیجه کې $5\mathbb{Z}$ فرعی ګروپ په $\mathbb{Z}$ کې دی.

تمرین 3.5: د 2.3 قضیی په اساس ثبوت کړی چې $11\mathbb{Z}$ او $6\mathbb{Z}$ فرعی ګروپونه په $(\mathbb{Z}, +)$ کې دي.

قضیه 3.6: هر فرعي ګروپ H په $(\mathbb{Z}, +)$ کې د $H = n\mathbb{Z}$ شکل لري . دلته $n\epsilon\mathbb{N}$ مساوي صفر اویا تر ټولو کوچنی طبیعي عدد په H کې دی .

ثبوت:

لمړی حالت : H={0}

$H=\{0\} \Rightarrow n = 0 \ \wedge\ H = \{0.a | a\epsilon\mathbb{Z}\} = 0\,.\mathbb{Z}$

دویم حالت : $H \neq \{0\}$

څرنګه چې H یو فرعي ګروپ د $\mathbb{Z}$ دی ، پس طبیعي اعداد هم په کې شامل دي.
مونږ فرضووچې n تر ټولو کوچنی طبیعي عدد په H کې دی.

$m\epsilon H \Rightarrow m\epsilon\mathbb{Z}$

$\Rightarrow \exists\ q, r\ \epsilon\mathbb{Z}; m = nq + r \quad 0 \leq r < n$ [division algorithm]

$\Rightarrow$ $r = m - nq\ \epsilon H$ [ځکه $m,n\ \epsilon H$]

څرنګه چې n ترټولو کوچنی طبیعي عدد په H کې دی ، پس باید r = 0 وې .

$\Rightarrow m = nq\ \epsilon H \Rightarrow H = n\mathbb{Z}$

تعریف 3.5 : یو عدد $c\in\mathbb{Z}$ مشترک قاسم (commen divisor) د $a_i \in \mathbb{Z}$ (i=1,....,n) اعدادو په نوم یادیږی ، پدي شرط چې ټول a_i پر c باندې قابل د تقسیم وي. یعنې:

$c \mid a_i \quad (i = 1,2,\ldots\ldots,n)$

تعریف 3.6: $a_1, a_2 \ldots\ldots, a_n \in \mathbb{Z}$ ، که $d, d_1, d_2 \ldots\ldots, d_k$ مشترک قاسم (commen divisor) د $a_n \in \mathbb{Z}$ (i=1,2,...n) وې او $d_i \mid d$ (i= 1,2,........,k) صدق وکړي . بیا d د $a_1, a_2 \ldots\ldots, an$ اعدادو د greatest commen divisor (ترټولو لوې مشترک قاسم) په نوم یادیږي او هغه په $d=\gcd(a_1, a_2 \ldots\ldots, an)$ سره ښیو.

قضیه 3.7 (Euclidean Algorithm) :

$a_1, a_2 \in \mathbb{Z}, a_1 \neq 0 \ \wedge\ a_2 \geq 1$

د پرله پسې ځوواره Division Algorithm استعمال څخه $a_3, a_4, \ldots\ldots \in \mathbb{Z}$ اعداد د لاندي خواصو سره لاس ته راغلې دي .

$a_1=q_1a_2+a_3 \qquad q_1\in \mathbb{Z}, 0 \le a_3< a_2$

$a_2 = q_2a_3+a_4 \qquad q_2\in \mathbb{Z}, 0 \le a_4 <a_3$

$\vdots \qquad \vdots \qquad (*)$

$a_{n-4} = q_{n-4}\, a_{n-3} +a_{n-2} \qquad q_{n-4}\in \mathbb{Z}, 0\le a_{n-2}<a_{n-3}$

$a_{n-3} = q_{n-3}\, a_{n-2} +a_{n-1} \qquad q_{n-3}\in \mathbb{Z}, 0\le a_{n-1}<a_{n-2}$

$a_{n-2} = q_{n-2}\, a_{n-1} +a_n \qquad q_{n-2}\in \mathbb{Z}, 0\le a_n<a_{n-1}$

$a_{n-1} = q_{n-1}\, a_n+ a_{n+1} \qquad q_{n-1} \in \mathbb{Z}, 0 = a_{n+1}$

په عمومي ډول کولای شو ولیکو:

$a_i = q_i . a_{i+1} + a_{i+2}, \qquad q_i \in \mathbb{Z}, 0 \le q_{i+2} < q_{i+1}$

قضیه وای چه یو n دلاندي خواصوسره موجود دی:

$\exists\, n \in \mathbb{N}, a_n \neq 0 \;\wedge\; a_{n+1} = 0 \;\wedge\; a_n = \gcd(a_1, a_2)$

ثبوت :

$a_2 > a_3 > \dots > 0 \quad \Rightarrow \quad \exists\, n \in \mathbb{N};\ a_n \neq 0 \;\wedge\; a_{n+1} = 0$

اوس پورتني معادلاي له لاندي پورته خوا ته مطالعه کوو :

$a_{n-1}= q_{n-1}\, a_n + a_{n+1} = q_{n-1}\, a_n + 0 \;\Rightarrow\; a_n \mid a_{n-1}$

$a_{n-2} = q_{n-2}\, a_{n-1} + a_n \;\wedge\; a_n \mid q_{n-2}\, a_{n-1}$ [$a_n \mid a_{n-1}$ ځکه]

$\wedge\; a_n \mid a_n$

$\Rightarrow\; a_n \mid a_{n-2}$

همدا ډول که وړانه دي ولاړ شو، بالاخره کولای شو چې ولیکو :

$a_n \mid a_{n-1} \Rightarrow a_n \mid a_{n-2} \Rightarrow \dots\dots \Rightarrow a_n \mid a_2 \;\wedge\; a_n \mid a_1$

په نتیجه کې a_n مشترک قاسم د a_1 او a_2 دی .

که t هم یو مشترک قاسم د a_1 او a_2 وي، بیا:

$t \mid a_1, a_2$

$a_1= q_1a_2 + a_3 \;\Rightarrow\; a_3 = a_1- q_1a_2$

$\Rightarrow t \mid a_3 \qquad$ [$t \mid a_2 \wedge t \mid a_1$ ځکه]

که همدارنګه ادامه ورکړو، بالاخره لاس ته راځي :

$t \mid a_1, a_2 \;\Rightarrow t \mid a_3 \;\Rightarrow \dots\dots \;\Rightarrow\; t \mid a_{n-1} \Rightarrow t \mid a_n$

له دي نتيجه کيږي چې a_n پر t قابل د تقسيم دی. پس a_n ترټولو لوی مشترک قاسم د a_1,a_2 دی. يعنې $a_n = gcd(a_1, a_2)$

اوس مو چې د a_2 ,a_1 مشترک قاسم a_n د Euclidean algorithm له لياری پيدا کړ، کولای شو $r,s\in \mathbb{Z}$ اعداد پيدا کړو چې لاندي معادله صدق کړي

$$a_n = ra_1 + sa_2$$

ددي لپاره د ($*$) معادلي څخه استفاده کوو.

$$a_{n-2} = q_{n-2} . a_{n-1} + a_n \Rightarrow a_n = a_{n-2} - q_{n-2} . a_{n-1}$$

له بلې خوا :

$$a_{n-3} = q_{n-3} . a_{n-2} + a_{n-1} \Rightarrow a_{n-1} = a_{n-3} - q_{n-3} . a_{n-2}$$

اوس د a_{n-1} پرځاې دهغه قيمت وضع کو

$$a_n = a_{n-2} - q_{n-2} . a_{n-1} = a_{n-2} - q_{n-2}(a_{n-3} - q_{n-3} . a_{n-2})$$

$$a_{n-4} = q_{n-4} . a_{n-3} + a_{n-2} \Rightarrow a_{n-2} = a_{n-4} - q_{n-4} . a_{n-3}$$

اوس د a_{n-2} پرځاې دهغه قيمت وضع کو

$$a_n = a_{n-2} - q_{n-2}(a_{n-3} - q_{n-3}\ a_{n-2})$$
$$= (a_{n-4} - q_{n-4} . a_{n-3}) - q_{n-2}(a_{n-3} - q_{n-3}\ (a_{n-4} - q_{n-4} . a_{n-3}))$$

که په همدا ډول ادامه ورکړو، په پورتنی معادله کې فقط a_1 او a_2 باقی پاتې کيږي چې د a_1 ضريب د r عدد او a_2 ضريب د s عدد دی. پس:

$$a_n = a_{n-2} - q_{n-2}(a_{n-3} - q_{n-3} . a_{n-2})$$
$$= (a_{n-4} - q_{n-4} . a_{n-3}) - q_{n-2}(a_{n-3} - q_{n-3}\ (a_{n-4} - q_{n-4} . a_{n-3}))$$
$$= \ldots\ldots\ldots = ra_1 + sa_2$$

مثال 3.1 : غواړود r او s اعداد پيداکړوچې لاندي رابطه صدق وکړي

$$gcd(9692,360) = r.9692 + s.360$$

حل:

9692 =26 . 360 + 332	4= 28 – 1 . 24
360 = 1 . 332 + 28	= 28-1(332-11.28)
332 = 11 . 28 + 24	= 12.28 – 1.332
28 = 1 . 24 + 4	= 12. (360-1 .332) -1 .332
24 = 6.4 + 0	= 12.360 – 13.332
	=12 . 360 – 13 .(9692-26.360)
	= 12.360 + 13.26(360) – 13.9692
	= 350 . 360 – 13 . 96 92

په نتيجه کې:

r = -13 , s = 350

gcd (9692 , 360) = 4 = (-13) . 96 96 + 350 .360

مثال: غواړو $r,s \in \mathbb{Z}$ پیدا کړو چې لاندي رابطه صدق کړي

gcd(-65,25) = r.(-65) + s25

حل:

-65 = -3.25 + 10 5 = 25 – 2.10
25 = 2.10 + 5 = 25 -2(-65 + 3.25)
10 = 2.5 + 0 = 25 + (-2).(-65) - 6.25
= (-2).(-65) + (-5).25

r = -2 , s = -5 , gcd(-65,25) = 5 **= -2**.(-65) + -5.25

تمرين 3.6: $r,s \in \mathbb{Z}$ په لاندي معادلوکي پیدا کړی :

(a) gcd(150,40) = r.150 + s.40
(b) gcd(170,30) = r.170 + s.30
(c) gcd(2615,315) = r.2615 + s.315
(d) gcd(-60,36)= r . (-60)+s.36

نوټ : که مونږ دري $a, b, c \in \mathbb{Z}$ اعداد ولرو، بیا دهغوي تروټولولوې مشترک قاسم (gcd) په لاندې ډول لاسته راځي :

$$\gcd(a,b,c) = \gcd(gcd(a,b)\,,c) = \gcd\,(a,\gcd(b,c))$$

که زیات شمیر اعداد ولرو، بیا هم دهغوي تروټولولوې مشترک قاسم (gcd) په همدي ډول لاسته راځي.

مثال 3.2: غوارو gcd(30,66,93) پیدا کړو .

Gcd(30, 66, 93) =gcd(gcd(30,66),93)
66= 2 .30 +6
30= 5 . 6 +0

پیدا شوچې gcd(30,66)=6

93= 15 .6 +3
6= 2.3+0

لیدل کیږي چې gcd(6 , 93) = 3 دی. پس:

Gcd(30,66,93) = gcd(gcd(30,66) ,93)

$= \gcd(6,93)=3$

مثال 3.3: غواړو gcd(36,60,150) پیداکړو .

لمړی gcd(36,60) پیده کو .

60=1.36+24

36=1.24+12

24=2.12+0

پس gcd(36, 60)= 12

gcd(12,150) = 6 دی. ځکه :

150 =12.12+6

12= 2.6+0

gcd(36,60,150) = gcd (gcd(36,60), 150)

= gcd(12,150) = 6

لیما 3.3: $a, b, c \in \mathbb{Z}$. بیا :

(a) $a \mid b.c \ \wedge \ \gcd(a,b) = 1 \Rightarrow a \mid c$

(b) $a \mid c \ \wedge \ b \mid c \ \wedge \ \gcd(a,b) = 1 \Rightarrow a.b \mid c$

(c) $\gcd(a,c) = 1 \ \wedge \ \gcd(b,c) = 1 \Rightarrow \gcd(a.b,c) = 1$

(d) $\text{P prime} \ \wedge \ p \mid a.b \ \Rightarrow p \mid a \ \vee \ p \mid b$

(a) ثبوت:

$$\gcd(a,b) = 1 \Rightarrow \exists\, r,s \in \mathbb{Z}\,; \text{ra} + \text{sb} = 1$$
$$\Rightarrow c.1 = rac + sbc$$
$$a \mid b.c \wedge a \mid a.c \Rightarrow a \mid rac + sbc \Rightarrow a \mid c$$

(b) ثبوت:

$$\gcd(a,b) = 1 \Rightarrow \exists\, r,s \in \mathbb{Z}\,; 1 = \text{ra} + \text{sb}$$
$$\Rightarrow c = rac + sbc$$

$$a \mid c \wedge b \mid c \Rightarrow ab \mid rac \wedge ab \mid sbc \Rightarrow ab \mid c$$

(c) ثبوت:

$\gcd(a,c) = 1 \Rightarrow r_1, s_1 \in \mathbb{Z};\ r_1 a + s_1 c = 1$

$\gcd(b,c) = 1 \Rightarrow \exists\, r_2 s_2 \in \mathbb{Z}\,; r_2 b + s_2 c = 1$

پورتنی معادلي له یو بل سره ضربو :

$r_1 r_2 ab + r_2 s_1 bc + r_1 s_2 ac + s_1 s_2 cc = 1$
$\Longrightarrow r_1 r_2 ab + (r_2\, s_1 b + r_1 s_2 a + s_1\, s_2 c).\, c = 1$
$m := r_1 r_2\ , n := r_2 s_1 b + r_1 s_2 a + s_1 s_2\ \in \mathbb{Z}$
$\Longrightarrow m(ab) + nc = 1 \Longrightarrow \gcd(ab, c) = 1$

ثبوت: (d) که a پر p باندې قابل د تقسیم نه وي. یعني p ∤ a

$P \nmid a \Longrightarrow \gcd(p,a) = 1 \Longrightarrow \exists\, r, s \in \mathbb{Z}\ , r.p + s.a = 1$
$\Longrightarrow b.\, r.p + b.s.a = b$

$p \mid brp \wedge p \mid bsa \Longrightarrow p \mid b$

تعریف 3.7 : طبعی عدد $d \in \mathbb{N}$ د ترټولوکوچنی مشترک مضرب (Lcm:= Least Commen Multiple) د $a_1, a_2, \dots, a_n \epsilon \mathbb{Z}$ اعدادو په نوم یادیږي په دي شرط چې :

(i) $a_i \mid d \quad \forall\ i \epsilon \{1,2,\dots,n\}$

که $s \in \mathbb{N}$ هم یو مشترک مضرب وی، بیا باید:

(ii) $a_i \mid s \quad \forall\ i \epsilon \{1,2,\dots,n\} \Rightarrow d \mid s$

Lcm د پیداکولولپاره لاندي طریقي موجودي دي

لمړی: د gcd او Lcm ترمینځه لاندي رابطه موجوده ده:

$m, n \in \mathbb{Z}$
$\gcd(m, n)\, .\, \mathrm{Lcm}(m, n) = |m.\, n|$

یعنی کولای شو Lcm د gcd له مخی پیداکړو

دویم: راکړل شوی اعداد په لمړنی فکتورو (factoring) تجزیه کول دي. دلته هغه شمیره چه په دواړوکی شامل اولوړطاقت ولری ا نتخابیږی اوبیا دمتباقی فکتورو سره ضربیږی

مثال : غواړو (Lcm(36,15 پیدا کړو

لمړی: د gcd له لیاری:

$m = 36\ \ , n = 15$
$36 = 2.15 + 6$
$15 = 2.6 + 3$
$6 = 2.3 + 0$
$\gcd\,(36,15) = 3$
$\gcd(36,15)\, .\, \mathrm{Lcm}(36,15) = |36.15|$

$$\Longrightarrow \mathrm{Lcm}(36,15) = \frac{540}{\gcd(36,15)} = \frac{540}{3} = 180$$

دویم: په لمړنی فکتورو (factoring) دتجزیی له لیاری

$36 = 2.2.3.3$
$15 = 3.5$

ځرنګه چې 3 په دواړوکې شامل دی،پس 3^2 په نظرکی نیسو

$Lcm(36,15) = 2.2.3.3.5 = 180$

مثال : غواړو (Lcm(72,108 پیدا کړو

$72 = 2^3 . 3^2$
$108 = 2^2 . 3^3$

ځرنګه چې 2 او 3 په دواړوکې شامل دی. پس 2^3 او 3^3 (ترټولوزیات طاقت لري) له یوبل دی سره ضرب کوواوحاصل يي ترټولوکوچنی مشترک مضرب (Lcm) دی .

مثال: غواړو (Lcm(-24,10 پیدا کړو

$m = -24 \ , n = 10$
$-24 = -3.10 + 6$
$10 = 1.6 + 4$
$6 = 1.4 + 2$
$4 = 2.2 + 0$
$gcd\,(-24,10) = 2$

$$Lcm(-24,10) = \frac{|-24.10|}{gcd(-24,10)} = \frac{240}{2} = 120$$

له بلی لیاری:

$-24 = 2^3.(-3)$
$10 = 2.5$

دمنفی علاموڅخه صرف نظرکوو. ځکه چه Lcm مثبت عدد تعریف شوی دی

$Lcm(-24,10) = 2^3.3.5 = 120$

مثال : غواړو (Lcm(8,10,12,16 پیداکړو

$8 = 2^3$
$10 = 2 . 5$
$12 = 2^2. 3$
$16 = 2^4$

ځرنګه چې د 2 عدد په ټولوکې شامل دی. پس 2^4 (یعني 2 ترټولولوړطاقت لري) د 3 او 5 سره ضرب کو. د دوې حاصل ضرب ترټولو کوچنی مشترک مضرب (Lcm) دی. یعني

Lcm(8,10,12,16) = 2^4. 3 . 5 = 240

تمرین 3.7 : Lcm(180 , 600) په دواړوطریقوپیداکړی

نوټ: د کوچني مشترک مضرب (Lcm) په کومک کولای شو په $(\mathbb{Z},+)$ کې د فرعی ګروپونو تقاطع پیدا کړو. یعنې که $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ او d دهغوي **ترټولو** کوچنی مشترک مضرب وې. بیا لاندي افاده صدق کوي :

$$d = Lcm(a_1, a_2, \ldots, a_n) \Rightarrow \bigcap_{i=1}^{n} a_i\mathbb{Z} = d\mathbb{Z}$$

ثبوت:

$$m \in d\mathbb{Z} \Rightarrow d \mid m \Rightarrow a_i \mid m \quad (i = 1,2,\ldots,n)$$
$$\Rightarrow m \in a_i\mathbb{Z} \quad (i = 1,2,\ldots,n) \Rightarrow m \in \bigcap_{i=1}^{n} a_i\mathbb{Z}$$
$$\Rightarrow d\mathbb{Z} \subseteq \bigcap_{i=1}^{n} a_i\mathbb{Z}$$

$$k \in \bigcap_{1=1}^{n} a_i\mathbb{Z} \Rightarrow k \in a_i\mathbb{Z} \quad (i = 1,2,\ldots,n)$$
$$\Rightarrow a_i \mid k \quad (i = 1,2,\ldots,n)$$
$$\Rightarrow d \mid k \quad (\text{d} = \text{Lcm}(\text{a1}, \text{a2}, \ldots, \text{an}) \text{ ځکه})$$
$$\Rightarrow k \in d\mathbb{Z} \Rightarrow \bigcap_{i=1}^{n} a_i\mathbb{Z} \subseteq d\mathbb{Z}$$

په نتیجه کې: $\bigcap_{i=1}^{n} a_i\mathbb{Z} = d\mathbb{Z}$

د مثال په ډول $2\mathbb{Z} \cap 3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$. ځکه :

Lcm(2,3,4) = 3 . 2^2 = 12

تمرین 3.8 :

(a) په $(\mathbb{Z},+)$ کې د $6\mathbb{Z}$, $10\mathbb{Z}$ او $4\mathbb{Z}$ فرعی ګروپوتقاطع پیدا کړی.

(b) په $(\mathbb{Z},+)$ کې د $6\mathbb{Z}$ او $8\mathbb{Z}$ فرعی ګروپو تقاطع کړی.

تعریف 3.8 : دیو (G,.) ګروپ دعناصروشمیرد group order (ګروپ مرتبه) په نوم یادیږي اوهغه په ord(G) او یا $|G|$ سره ښیو. که ګروپ معین نه وې، بیا هغه په ord (G) = ∞ سره ښیو.

د مثال په ډول د $(\mathbb{Z},+)$ مرتبه غیرمعین او $ord(A^{(4)}) = 4$ ده

نوټ : په یو $(G, \oplus)$ ګروپ کې د آساني لپاره د $a \oplus a \oplus \ldots\ldots \oplus a$
(m واري (دفعه)) پرځای a^m لیکو .

تعریف 3.9 : $(G, \oplus)$ یو ګروپ ، e عینیت عنصر (خنثی) او $a \in G$ دی.
ترټولو کوچنی $m \in \mathbb{N}$ چې $a^m = e$ شي د order a (مرتبه) په نوم یادیږي
او مونږ هغه په $ord_G(a)$ ښیو. یعنې:

$$ord_G(a) = \min \{i \in \mathbb{N} \mid a^i = e\}$$

که معلوم وي چې کوم ګروپ هدف دی. بیا فقط $ord(a)$ لیکو .
د مثال په ډول $ord(D_4,.) = 8$

$e^1 = e \Rightarrow ord(e) = 1$

$b.b = b^2 = e \Rightarrow ord(b) = 2$

$c.c = b$

$c^3 = c.c.c = b.c = a$

$c^4 = c.c.c.c = a.c = e \Rightarrow ord(c) = 4$

تمرین 3.9: $ord(d)$ ، $ord(f)$ او $ord(g)$ په $(D_4,.)$ او $(Q_8,.)$
ګروپوکې پیدا کړی.

قضیه 3.8 : $(G, \odot)$ یو معین ګروپ ، $a \in G$ او e عینیت عنصر دی. بیا د
a مرتبه (order) د G د مرتبې (order) څخه کوچني یا مساوی ده . یعنې:

$$ord(a) \leq ord(G)$$

ثبوت : $|G| = ord(G)$, $k = ord(a)$
که $ord(a) \leq ord(G)$ نه وي. په دې صورت باید $k > |G|$ او
$k \geq |G|+1$ شي.

$X := \{1,2,3,\ldots\ldots k\}$

$f : X \longrightarrow G$

$i \longmapsto a^i$

څرنګه چې $k > |G|$ فرض شوی دی، پس باید $i, j \in X$ د لاندې خواصوسره
موجود وي.

$i > j$, $f(i) = a^i = f(j) = a^j \Rightarrow a^i . (a^j)^{-1} = a^j (a^j)^{-1}$

$\Rightarrow a^{i-j} = e$

له دې څخه نتیجه اخلو چې $ord(a)$ مساوی د $i - j$ کیږي . مګردا د مرتبې
(order) د تعریف سره تضاد لري . ځکه k ټولو کوچنی عدد دی چې $a^k = e$
شي. مګردلته $0 < i - j < k$ دی. پس باید $Ord(a) \leq ord(G)$ وي.

قضیه 3.9 (theorem of fermat) **:** $(G, .)$ یو معین ګروپ , e عینیت
عنصر او $a \in G$. بیا $a^{ord(G)} = e$

ثبوت : څرنګه چې G معین ګروپ دی. پس کولای شو ولیکو:

$G = \{ g_1, g_2, \ldots, g_n \}$, $ord(G) = |G| = n$

مونږپر G بانه دي دا لاندي تابع په نظرکي نيسو :

$$f: G \longrightarrow G$$
$$g \longmapsto a.g$$

غواړو ثبوت کړو چې f يو bijective دی.

$$x, y \in G, f(x) = a.x = f(y) = a.y$$
$$ax = ay \Rightarrow a^{-1}.a.x = a^{-1}.a.y \Rightarrow x = y \Rightarrow f \ \ injective$$

څرنګه چه G متناهی ګروپ دی، پس د 0.1 قضيي له مخی سوريکتيف هم دی.اويا په لاندي شکل:

$$\forall \in G, x: = a^{-1}.y \Rightarrow f(x) = (a^{-1}.y) = a.(a^{-1}.y) = y$$
$$\Rightarrow f \ surjective$$

ثبوت شو چې f يو bijective دی. پس:

$$G = f(G) \Rightarrow \{g_{1,}g_2, \dots, g_n\} = \{ag_{1,}ag_2, \dots, ag_n\}$$

$$\Rightarrow \prod_{i=1}^{n} g_i = \prod_{i=1}^{n} ag_i = a^n \prod_{i=1}^{n} g_i$$

$$\Rightarrow (\prod_{i=1}^{n} g_i) . (\prod_{i=1}^{n} g_i)^{-1} = a^n (\prod_{i=1}^{n} g_i) . (\prod_{i=1}^{n} g_i)^{-1}$$

$$\Rightarrow a^n = e \quad \Rightarrow \quad a^n = a^{ord(G)} = e$$

قضيه 3.10 : $(G, .)$ يو معين ګروپ چې e دهغه عينيت عنصراو $a \in G$ وي. بيا ord(G) پر ord(a) باندي قابل د تقسيم ده . يعني ord(a)| ord(G) .

ثبوت : که ord(G) = m او ord(a) = n وي اومونږفرض کړو چې ord(G) پرord(a) بانه دي قابل د تقسيم نه ده. بيا په دي صورت:

$$\exists\ q,r \in \mathbb{N}\ ;\ m=q.n+r \qquad (\ 0< r < n\ )$$
$$\Rightarrow r = m-q.n$$

د fermat قضيي له مخې پوهيږو چې $a^{ord(G)} = a^m = e$ ده. پس:

$$a^r = a^{m-qn} = a^m . (a)^{-qn} = a^m . (a^n)^{-q} = e.(e)^{-q} = e.(e^q)^{-1} = e$$

مګردا د مرتبي (order) د تعريف سره تضاد لري . ځکه n ترټولو کوچنی عدد دی چې $a^n = e$ شي. پورته مګروليدل شو چې $a^r = e$ او r < n دی. پس بايد ord(a)| ord(G) وي.

ليما 3.4 : هرګروپ چې دهغه مرتبه (order) يو اوليه عدد وي ، بيا هغه ګروپ دورانی (cyclic group) دی.

ثبوت : که (. ,G) یو ګروپ وي چې مرتبه (order) یي اولیه عدد p او e دهغه عینیت عنصر وې .
که {e} = G وي، بیا د G دورانی توب واضح دی.
اوس فرضووچې G ≠ {e} دی.

$$G \neq \{e\} \Rightarrow \exists\, a \in G, a \neq \{e\}$$

$$\text{ord}(G) = p \;\Rightarrow\; \text{ord}(a) \mid p \quad [\text{ قضیی له مخی } 3.10 \;]$$

څرنګه چې p اولیه عدد دی. پس باید ord(a) = p وي او په نتیجه کې G= <a> صدق کوی. یعنې G یو دورانی ګروپ دی .

مثال 3.4 : په $(A^{(4)},\oplus)$ ګروپ کې عینیت عنصر a_0 دی

$$\text{ord}(A^{(4)}) = |A^{(4)}| = 4$$

$$a_1 \oplus a_1 = a_2$$

$$a_1 \oplus a_1 \oplus a_1 = a_2 \oplus a_1 = a_3$$

$$a_1 \oplus a_1 \oplus a_1 \oplus a_1 = a_3 \oplus a_1 = a_0 \quad \Rightarrow a_1^4 = a_0$$

$$\Rightarrow \text{ord}(a_1) = 4 \quad \wedge \quad \text{ord}(a_1) \mid \text{ord}(A^{(4)})$$

$$a_2 \oplus a_2 = a_0 \quad \Rightarrow a_2^2 = a_0$$

$$\Rightarrow \text{ord}(a_2) = 2 \quad \wedge \text{ord}(a_2) \mid \text{ord}(A^{(4)})$$

$$a_3 \oplus a_3 = a_2$$

$$a_3 \oplus a_3 \oplus a_3 = a_2 \oplus a_3 = a_1$$

$$a_3 \oplus a_3 \oplus a_3 \oplus a_3 = a_3 \oplus a_1 = a_0 \Rightarrow a_3^4 = a_0$$

$$\Rightarrow \text{ord}(a_3) = 4 \;\wedge \text{ord}(a_3) \mid \text{ord}(A^{(4)})$$

همدارنګه لیدل کیږي چې $\text{ord}(a_1), \text{ord}(a_2), \text{ord}(a_3) \leq \text{ord}(A^{(4)})$

تمرین 3.10:

(a) ord(E),ord(K), ord(-E),ord(I) په (Q,.) ګروپ کې پیدا کړی.

(b) ord(f) ,ord(h) , ord(g) په (.,Q_8) ګروپ کې پیدا کړی.

(c) : $(G, *)$ یو معین ګروپ چې عینیت عنصریی e دی. a∈ G

$$\varphi: (\mathbb{Z}, +) \longrightarrow (G, *)$$
$$n \longmapsto a^n$$

ثبوت کړی چې φ یو G-Hom دی او ker(φ) پیدا کړی

تعریف 3.10 : $(G, \oplus)$ یو ګروپ او H دهغه یوفرعی ګروپ دی. a ∈ G

$a \oplus H=\{a\oplus h \mid h\in H\}$ د left coset (چپ کلاس) او

$H\oplus a =\{h\oplus a \mid h\in H\}$ د right coset (ښی کلاس) په نوم یادیږي

مثال : مونږ په $A^{(2.2)}$ کې د $H:=\{b_1, b_2\}$ فرعي ګروپ په پام کې نیسو

$b_1 \odot H = \{b_1 , b_2 \}$
$b_2 \odot H = \{b_2, b_1\}$
$b_3 \odot H = \{b_3, b_4\}$
$b_4 \odot H = \{b_4, b_3\}$

لیدل کیږي:

$H_1 := b_1 \odot H = b_2 \odot ,\quad H_2 := b_3 \odot H = b_4 \odot H$

دټولو left-coset (چپ کلاسو) شمیر په $A^{(2.2)}$ کې نظر H ته 2 دی همدارنګه لیدل کیږي چې :

$A^{(2.2)} = H_1 \cup H_2$

قضیه 3.11 : (G, .) یو ګروپ ، U د هغه فرعی ګروپ او a,b∈G دی. بیا:

(a) a.U = U ⇔ a∈ U
(b) a.U = b.U ⇔ a^{-1}.b∈U
(c) a.U∩b.U≠ ∅ ⇔ a.U =b.U

(په دي معنی چې دوه left-coset یا سره مساوی دي اویا خالی تقاطع لري)

(a) ثبوت :

"⇐"

g∈ aU ⇒ ∃ u∈U ; g=a.u
⇒ g∈U [a,u ∈ U ځکه U فرعی ګروپ او]
⇒ aU ⊆ U
g∈ U ⇒ g = e.g = a. a^{-1}.g = a.(a^{-1}.g)
⇒ g ∈aU [a ,g ∈U ځکه]

په نتیجه کې aU = U g

"⇒"

g∈ aU = U ⇒ ∃ u∈U ; g = a.u , g.u ∈ a.U = U
⇒ a = g. u^{-1} ⇒ a∈U [g,u∈ U ځکه]

(b) ثبوت:

"⇐"

a^{-1}.b ∈ U ⇒ a^{-1} . b . U = U [د (a) له مخې]
⇒ a. a^{-1} . b . U = a . U
⇒ b .U = a .U

"⇒"

g∈ aU = bU ⇒ u_1 ,u_2∈ U; g = a.u_1 = b.u_2
⇒ a^{-1} .a.u_1. ${u_2}^{-1}$ = a^{-1}. b u_2. ${u_2}^{-1}$
⇒ u_1. ${u_2}^{-1}$ = a^{-1}.b
⇒ a^{-1}.b ∈U [u_1, u_2 ∈U ځکه]

(c) ثبوت:

„ ⇐”

$g\in a.U = b.U$

$\Rightarrow \exists\ u_1, u_2 \in U ; g = a.u_1 = b.u_2$

$\Rightarrow g \in a.U \cap b.U$ [ځکه $a.u_1 \in a.U$ او $b.u_2 \in b.U$ دی]

په نتیجه کې $a.U \cap b.U \neq \emptyset$

„⇒ "

$a.U \cap b.U \neq \emptyset \Rightarrow \exists\ g \in aU \cap bU$

$\Rightarrow \exists\ u_1, u_2 \in U; g = a.u_1 = b.u_2$

$\Rightarrow a^{-1}.a.u_1.u_2^{-1} = a^{-1}b.u_2.u_2^{-1}$

$\Rightarrow u_1 . u_2^{-1} = a^{-1}.b \Rightarrow a^{-1}.b \in U$ [ځکه $u_1, u_2 \in U$]

$\Rightarrow a.U = b.U$ [د (b) له مخې]

لیما 3.5 : (G,.) یو ګروپ او U د هغه فرعی ګروپ دی . بیا:

(1) $G = \bigcup_{a\in G} aU$, په دې شرط چې هردوه left-coset سره مساوی اویا خالی تقاطع ولري .

(2) $a\in G$

$|a.U|=|U|=|Ua|$

(یعني د هر $a \in G$ لپاره د U ، U.a او a.U د عناصرو شمیر سره مساوی دی)

(1) **ثبوت:** $\bigcup_{a\in G} aU \subseteq G$ واضح دی.

$\forall a\in G$, $a=a.e \in a.U$ [ځکه $e \in U$]

$\Rightarrow G \subseteq \bigcup_{a\in G} aU$

په نتیجه کې $G = \bigcup_{a\in G} aU$

د 3.11 قضیې له مخې هردوه left- coset (چپ کلاس) یا به سره مساوی اویا متقاطع یې خالی ده . یعني د $a,b\in G$

$a.U \cap b.U \neq \emptyset \Leftrightarrow a.U = b.U$

(2) ثبوت: د $a\in G$ لپاره لاندې تابع تعریفوو:

$f:U \longrightarrow aU$

$u \mapsto a.u$

f یو bijective دی. ځکه :

$u_1, u_2 \in U ; f(u_1) = au_1 = au_2 = f(u_2)$

$\Rightarrow u_1 = a^{-1}.a\, u_2 = u_2 \Rightarrow$ injective

$b\in aU \Rightarrow \exists\ u\in U; b = a.u = f(u) \Rightarrow f$ surjective

څرنګه چې f یو bijective دی پس د U او aU عناصرو شمیرسره مساوی دی. یعنې $|aU| = |U|$

همدا ډول کولای شو ثبوت کړو چې لاندي تابع هم bijective ده .

f :U ⟶ Ua
u ⟶ u.a

په نتيجه کي $|aU|$=$|U|$=$|Ua|$

مثال: په $(Q_8,.)$ ګروپ کې H= {e,a,g,h} يو فرعي ګروپ دی او $b\in Q_8$ په نظرکې نيسو

b.H = b.{e,a,g,h} = { b,c,f,d} ⟹ $|b.H|$ = 4 = $|H|$

اوس غواړو وښيو:

$Q_8 = \cup_{a\in Q_8} aH$

د 3.11 قضی له مخې پوهيږو چې:

e,a,g,h$\in H$ ⟹ e.H = a.H = g.H = h.H = H

اوس د Q_8 پاتي عناصرپه نظرکې نيسو

b.H = b.{e,a,g,h} = { b,c,f,d}
c.H = c.{e,a,g,h} = { c,b,d,f}
d.H = d.{e,a,g,h} = { d,f,b,c}
f.H = f.{ e,a,g,h } = { f,d,c,b }

ليدل کيږي چې :

U:=b.H = c.H = d.H = f.H

په نتيجه کې:

$Q_8 = H \cup U$

مثال 3.5 : که مونږ د U = 6ℤ فرعی ګروپ په (+, ℤ) کې په نظرکې ونيسو ، ليدل کيږي چې

5+6 ℤ , 4+6 ℤ , 3+6 ℤ ,2+6 ℤ , 1+6 ℤ , 6 ℤ

Left-cosets (چپ کلاسو) نظر U ته دي چې دټولوعناصرو شميرديوبل سره مساوی دي . د مثال په ډول د 3. 5 ليما له مخې $|6\mathbb{Z}|$= $|3 + 6\mathbb{Z}|$ مګر هغه ټول Left-coset له يوبل څخه مختلف دي. ځکه :

U=6 ℤ ={. . . -18 , -12 , -6 , 0 , 6 , 12 , 18 . . .}
1+6 ℤ ={. . . -17 , -11, -5 , 1 , 7 , 13 , 19 . . .}
2+6 ℤ ={. . . -16 , -10 , -4 , 2 , 8 , 14 , 20. . .}

1+6 ℤ او 7+6 ℤ سره مساوی دي. ځکه

7+6 ℤ = 1+(6+6 ℤ)= 1+6 ℤ [د 3.11 قضيي له مخې]

تعریف 3.11 : (G , .) یو گروپ او U فرعی گروپ په G کې دی .
U د ټولومختلفو leftcoset په G کې د Index په نوم یادیږي اوهغه په
ind $_G$ (U) اویا [G : U] ښودل کیږي . یعني

$$\text{ind}_G(U) = |\{a.U \mid a \in G\}| = |U.a \mid a \in G| = [G:U]$$

مثال :
(a)

$$\text{ind}_G(G) = |G:G| = 1 , \quad \text{ind}_G(e) = [G:\{e\}] = |G|$$

(b)

$$\text{ind}_{\mathbb{Z}}(n\mathbb{Z}) = [\mathbb{Z} : n\mathbb{Z}] = n \ \forall \ n \in \mathbb{N}$$

ځکه ټول چپ کلاسونه د $n\mathbb{Z}$ په $\mathbb{Z}$ کې مساوی n دي . د مثال په ډول په $5\mathbb{Z}$ فرعی
گروپ کې $\text{ind}_{\mathbb{Z}}(5\mathbb{Z}) = [\mathbb{Z} : 5\mathbb{Z}] = 5$

قضیه 3.12 : $(G,.)$ یو معین گروپ ، H او H_1 فرعی گروپونه په G کې او
$H_1 \subseteq H$ دی بیا:

$[G:H_1]=[G:H].[H:H_1]$ (یعني $\text{ind}_G(H_1) = \text{ind}_G(H).\ \text{Ind}_H(H_1)$)

ثبوت: د 3.5 لیما له مخې کولای شو G په لاندي شکل ولیکو:

$$G = \cup_{i\in I} a_i H$$

$a_i \in G$ دا ډول انتخاب شوي دي چې د H-left coset په اتحاد کې یوچپ
کلاس دوه دفعه ظاهر نه شي. یعنې ټول a_iH یوله بل څخه فرق لري اوپه نتیجه
کې I = [G:H] .
په همدې ډول کولاي شوولیکو :

$$H = \cup_{j\in J} b_j H_1$$

دلته هم $b_j \in H$ دا ډول انتخاب شوي چې د H_1-leftcoset په اتحاد کې
یوچپ کلاس دوه دفعه ظاهر نه شي. یعنې ټول b_jH_1 یوله بل څخه فرق لري
اوپه نتیجه کې $J = [H:H_1]$

$$G = \cup_{i\in I} a_i H = \cup_{i\in I} a_i (\cup_{j\in J} b_j H_1) = \cup_{i\in I}\left(\cup_{j\in J} a_i b_j H\right)$$

$$\Longrightarrow \quad [G:H_1] = I.J$$

$$\Longrightarrow [G:H_1] = I.J = [G:H].[H:H_1]$$

مثال: $\{b_1\}$ $H_1=$ او $H=\{b_1,b_4\}$ فرعی گروپونه په $(A^{(2,2)},\odot)$ کې دي.
ځرنګه چې b_1 عینت عنصر د $A^{(2,2)}$ دی. پس ټول leftcoset د H_1 نظر $A^{(2,2)}$ ته $\{b_1\},\{b_2\},\{b_3\}$ او $\{b_4\}$ دي.

یعني $ind_{A(2,2)}(H_1) = 4$

$b_2\odot H = b_2\odot \{b_1,b_4\} = \{ b_2\odot b_1, b_2\odot b_4\} = \{b_2,b_3\}$
$b_3\odot H = b_3\odot \{b_1,b_4\} = \{ b_3 \odot b_1, b_3\odot b_4\} = \{b_3,b_2\}$

د H ټول leftcoset نظر $A^{(2,2)}$ ته $\{b_1,b_4\}$ **او** $\{b_2,b_3\}$ دي اوپه نتیجه کې $ind_{A(2,2)}(H) = 2$. د H_1 ټول leftcoset نظر H ته $\{ b_1 \}$ او $\{b_4\}$ دي. یعني $Ind_H(H_1) = 2$

$ind_{A(2,2)}(H_1) = 4 = 2.2 = ind_{A(2,2)}(H) . Ind_H(H_1)$

اویا به بل شکل:

$[G:H_1]= 4=2.2 =[G:H].[H:H_1]$

قضیه 3.13: (Lagrange) $(G,.)$ یومعین ګروپ ، e د هغه عینیت عنصر (identity) او H یو فرعی ګروپ په G کې دی. بیا :

$$Ord(G)= ord(H) . ind(H)$$

ثبوت: که $E := \{e\}$ تعریف شي. بیا E فرعی ګروپ د G او H دی. پس:

$Ord(G) = [G:E] \quad \wedge \quad ord(H) = [H:E]$

اویا په بل شکل

$$|G| = \mathrm{ind}_G(E) \qquad \wedge \qquad |H| = \mathrm{ind}_H(E)$$

پس د 3.12 قضیې له مخې کولاشوولیکو:

$$ord(G) = [G:E] = [G:H] . [H:E] = [G:H] . ord(H)$$

نوټ: د **Lagrange** قضیې څخه نتیجه اخلوچې د یو معین ګروپ مرتبه (order) پرمرتبه دهغه هر فرعی ګروپ قابل د تقسیم ده.

مثال: $H=\{e,a,d,f\}$ یوفرعی ګروپ په Q_8 کې دی . غواړو $Ind_{Q_8}(H)$ پیدا کړو.

ځرنګه چې $ord(H) = 4$ او $ord(Q_8) = 8$ دی. پس د **Lagrange** قضیې له مخې لیکلی شو

$ord(Q_8) = ind(H). ord(H) \Rightarrow 8 = ind(H). 4$

$\Rightarrow$ ind(H) = $\frac{8}{4}$ = 2

تمرين 3.11 :

(a) په (D_4,.) ګروپ کي {e,b} = H_1 او H = {e,a,b,c} فرعی ګروپونه دي.

(i) $Ind_{D_4}(H_1)$, $ind_{D_4}(H)$, $ind_H(H_1)$ پيداکړی.

(ii) مربوطه left-coset يی معلوم کړئ. يعني دلاندي سيتو عناصر پيداکړي.

$\{a.H \mid a \in G\}, \{a.H_1 \mid a \in G\}, \{a.H_1 \mid a \in H\}$

(b) (G,.) يو ګروپ دی ، H_1 او H د G فرعي ګروپونه دي ، $H_1 \subseteq H$ ، $ind_G(H) = 6$, $ind_H(H_1) = 4$. معلوم کړئ چې د H_1 د left-coset شمير نظر G ته څودی . يعني $ind_G(H_1)$ پيداکړی .

(c) مونږ دا لاندي (G,.) ګروپ لرو:

G = { a, a^2,a^3,....,a^{14},a^{15}, a^{16} = e } ,
H = { a^4 , a^8 , a^{12} , a^{16} = e} , H_1 = { a^8 , a^{16} = e}

(i) ثبوت کړئ چې H او H_1 دوراني فرعي ګروپونه د G دي

(ii) $ind_G(H)$ او $ind_G(H_1)$ پيدا کړئ

مثال 3.5: د S_3 ګروپ دعناصرو شمير 6 دی. ځکه

$|S_3|$= 3! = 1.2.3=6

اوس هغه 6 عناصروته لاندي نومونه ورکوو :

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} , \ f_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} , \ f_2 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$f_3 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} , \ f_4 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} , \ f_5 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

پس S_3={ id ,f_1,f_2,f_3,f_4,f_5}

د 3.4 قضيي له مخې S_3 نظرد تابع ترکيب (Map composition) يوګروپ دی او (S_3, o) کيلی جدول (Cayley Table) لاندي شکل لري :

0	id	f_1	f_2	f_3	f_4	f_5
id	id	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_3	f_4	id	f_5	f_2
f_2	f_2	f_5	id	f_4	f_3	f_1
f_3	f_3	id	f_5	f_1	f_2	f_4
f_4	f_4	f_2	f_1	f_5	id	f_3
f_5	f_5	f_4	f_3	f_2	f_1	id

د مثال په ډول په پورتني جدول کې $f_3 \circ f_4 = f_2$ کيږي.

$$f_3 \circ f_4 = \begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix} = f_2$$

اويا په مفصل شکل :

$f_4(1)=2$, $f_4(2)=1$, $f_4(3)=3$

$f_3 \circ f_4(1) = f_3(2) = 1$, $f_3 \circ f_4(2) = f_3(1) = 3$,

$f_3 \circ f_4(3) = f_3(3) = 2$

پس $f_3 \circ f_4 = \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix} = f_2$

څرنګه چې $|S_3|=6$ دی پس د Lagrange قضيي له مخې S_3 يوازې هغه ډول فرعی ګروپونه درلودلی شي چې مرتبه (order) يې 1,2,3 و 6 وي. ځکه 6 پرهمدي اعدادو د ويش وړ(قابل د تقسيم) دی .

نوټ: د $(S_3,\circ)$ ګروپ ځيني مشخصات :

(a) S_3 دا لاندې فرعی ګروپونه لري .

(1) {id} چې مرتبه (order) يې 1 دی .

(2) S_3 چې مرتبه (order) يې 6 دی .

(3)

$U_1 := \langle f_2 \rangle = \{id , f_2\}$, $U_2 := \langle f_4 \rangle = \{id, f_4\}$, $U_3 := \langle f_5 \rangle = \{id, f_5\}$

ټول دا فرعی ګروپونه دورانی (cyclic) دي او

$ord(U_1) = ord(U_2) = ord(U_3) = 2$

دمثال په ډول ښيو چې U_3 دوراني فرعی ګروپ دی. ځکه که جدول ته وګورو

$id \circ id = id$, $id \circ f_5 = f_5$, $f_5 \circ f_5 = id$

له بلې خوا ليدل کيږي چې f_5 د U_3 مولد دی. يعنې $\langle f_5 \rangle = U_3$

$Ord(U)=3$ ، $U:=\langle f_1\rangle=\{id, f_1, f_3\}$ (4)

(b) که H یو فرعی ګروپ په S_3 کې وي. دپورتنیو فرعی ګروپو Index (ټولو left costes شمیر) کولای شو د Lagrange قضیي له مخې په لاندي ډول پیداکړو :

$|S_3| = |H| .[S_3:H]$

اویا

$ord(S_3) = \text{ord}(H) . \text{ind}(H)$

$\text{ind}(\{id\}) = \frac{|S_3|}{|\{id\}|} = \frac{6}{1} = 6$

$\text{ind}(S_3) = \frac{|S_3|}{|S_3|} = \frac{6}{6} = 1$

$\text{ind}(U_1) = \text{ind}(U_2) = \text{ind}(U_3) = \frac{|S_3|}{2} = \frac{6}{2} = 3$

$\text{ind}(U) = \frac{|S_3|}{|U|} = \frac{6}{3} = 2$

اوس غواړوټول left coset (چپ کلاسونه) د U_3 پرته د lagrange قضیي محاسبه کړو.

څرنګه چې $U_3 = \{id, f_5\}$ دی . پس په S_3 ګروپ کې لاندي امکانات موجود دي .

U_3 , $f_1 o\, U_3$, $f_2 o\, U_3$, $f_3 o\, U_3$, $f_4 o\, U_3$

$f_1 o\, U_3 = f_1 o \{id , f_5\} = \{ f_1 o\, id , f_1 o\, f_5\} = \{ f_1, f_2\}$

$f_2 o\, U_3 = f_1 o \{id , f_5\} = \{ f_2 o\, id , f_2 o\, f_5\} = \{ f_2, f_1\}$

لیدل کیږي چې $f_3 o\, U_3 = f_2 o\, U_3$

$f_3 o\, U_3 = f_3 o \{id , f_5\} = \{ f_3 o\, id , f_3 o\, f_5\} = \{ f_3, f_4\}$

$f_4 o\, U_3 = f_4 o \{id , f_5\} = \{ f_4 o\, id , f_4 o\, f_5\} = \{ f_4, f_5\}$

دلته لیدل کیږي چې $f_3 o\, U_3 = f_4 o\, U_3$

بالآخره نتیجه اخلوچې د left coset (چپ کلاسو) د U_3 په S_3 کې مساوی 3 دی.د Lagrange له لیاري هم دغه نتیجه لاس ته راغلي وه .

تمرین 3.12 :

(a) ثبوت کړئ چې په 3.5 مثال کې $\langle f_1\rangle = \{id , f_1 , f_3\}$ صدق کوي

(b) f_3 په S_3 کې مولد د کوم فرعی ګروپ کیدای شي .

(c) ثبوت کړئ چې $H: :=\{f\epsilon\, S_4 \mid f(4) = 4\}$ یو فرعی ګروپ د S_4 دی. $|H|$ او ind(H) پیدا کړئ .

مثال 3.6 : د 1.7 په مثال کې موولیدل چې $Q := \{\pm E , \pm I , \pm J ,\pm K\}$
نظرد ضرب د ماتریکس یو ګروپ او E د هغه عینیت عنصردی. په اسانی سره
ښودلای شو چې $H:= \{E,-E,I,-I\}$ یو فرعی ګروپ د Q دی.
H یو دورانی ګروپ هم دی چې د I متریکس دهغه موٴلد دی. ځکه
$I^2 = I.I = -E \quad , \quad I^3 = I.I.I = = -E.I = -I \quad , I^4 = I^3 . I = -I.I = E$
په نتیجه کې $H = <I>$ او $ind(H)$ مساوی 2 دی.

$$[Q: H] = [Q:<I>] = \frac{\mathrm{ord}(Q)}{\mathrm{ord}(<I>)} = \frac{8}{4} = 2$$

تعریف 3.12: $(G ,.)$ یو ګروپ او N فرعی ګروپ د G دی. N ته نورمال (normal) اویا invariant ویل کیږي، په دي شرط چې $a .N=N .a$ د هر $a\epsilon G$ لپاره وي . مونږ هغه په $N \trianglelefteq G$ ښیو .

مثال

(a) e د (G,.) ګروپ عینیت عنصر دی. {e} نورمال Normal په G دی . ځکه $\forall a\epsilon G$

$$a .\{e\} a^{-1} =\{e\} \Rightarrow a.\{e\}= \{e\} .a$$

(b) د تبدیلی (commutative) ګروپ هر فرعی ګروپ نورمال (normal) دی .

لیما 3.6: که (G ,.) یو ګروپ او N د هغه یو فرعی ګروپ وي . بیا :
$\forall a\epsilon G; a.N\, a^{-1} \subseteq N \quad \Leftrightarrow \quad$ ($N \trianglelefteq G$ یعنې N نورمال په G)
ثبوت : " $\Leftarrow$ "

$$N \trianglelefteq G \;\Rightarrow\; \forall a\epsilon G;\; aN = Na$$
$$\Rightarrow \forall x\epsilon N;\; a.x = x.a \;\Rightarrow\; a.x.a^{-1} = x$$
$$\Rightarrow a.x\,.\,a^{-1}\epsilon N$$

ثبوت " $\Rightarrow$ "

$$\forall a\epsilon G;\; a.N\,.\,a^{-1} \subseteq N \;\wedge\; a^{-1}\, N\, a \subseteq N$$

$$\Rightarrow\; aN \subseteq Na \;\wedge\; Na \subseteq aN$$

$$\Rightarrow aN = Na \quad \Rightarrow N \trianglelefteq G$$

له دي لیما څخه نتیجه اخلوچې په خپله G هم نورمال(Normal) په G کې دی ځکه $a\epsilon G$:

$$\forall g\epsilon G;\; a.g\,.\,a^{-1} \epsilon\, a\, G\; a^{-1}$$

له بلې خوا $a.g\,.\,a^{-1}\epsilon G$ هم دی. پس $a.G\,.a^{-1}\subseteq G$

مثال 3. 7:

(a) مونږ په 3.5 مثال کې ولیدل چې $U3:=<f5> = \{id ,f5\}$ یو فرعی

گروپ په S_3 کې دی. . مګر نورمال نه دی :

$f_1\circ U_3 = \{ f_1\circ id , f_1\circ f_5\} = \{ f_1, f_2\}$

$U_3\circ f_1=\{id\circ f_1 , f_5\circ f_1\}= \{f_1 , f_4\}$

څرنګه چې $f_1\circ U_3 \neq U_3 \circ f_1$ دی. پس U_3 نورمال (Normal) نه دی.

(b)

$N:= \{ A \in (GL(2,\mathbb{R}),.) \mid detA = 1 \}$

په 3.A مثال کی مووليدل چې N يو فرعی ګروپ د $GL(2,\mathbb{R})$ دی. اوس غواړو ثبوت کړوچې N نورمال په $GL(2,\mathbb{R})$ کی دي .

$A\in N , B\in (GL(2,\mathbb{R}),.) \Rightarrow detA = 1 , detB\neq 0$

$$\det(B.A.B^{-1}) = \det B . \det A . \det(B^{-1}) = \det B . \det A . \frac{1}{\det B}$$

$$= \det B . \frac{1}{\det B} . \det A = \det A = 1$$

$\Rightarrow B . A . B^{-1} \in N$

په نتيجه کی N د 3.6 ليما له مخی نورمال په $(GL(2,\mathbb{R}),.)$ کی دی

تمرين 3.13 : ايا $U_1 := \{id , f_1, f_3\}$ په 3.5 مثال کې يو فرعی نورمال ګروپ دی .

تعريف 3.13 : $(G , .)$ يو ګروپ او $A,B \subseteq G$

$A.B:=\{ a.b \mid a\epsilon A , b\epsilon B \}$

A.B د complex product په نوم ياديږي .

$A^{-1}:=\{ a^{-1} \mid a\epsilon A \}, \quad a.B:=\{a\}.B , \quad A.b := A\{b\}$

مثال: که مونږ په Q_8 ګروپ کې د $B :=\{a,f,g,h\}$ ، $A:=\{a,b,d\}$ فرعي سيټونه په نظرکې ونيسو :

$A.B = \{a,b,d\} . \{a,f,g,h\}$

$= \{ a.a, b.a, d.a, a.f, b.f, d.f, a.g, b.g , d.g,a.h, b.h, d.h \}$

$= \{ e, b, c, d, f , g, h \}$

$A^{-1} = \{ a^{-1}, b^{-1}, d^{-1}\} = \{ a, c, f \}$

تمرين 3.14: $B:= \{ e, b,f, h \},A:=\{ a, b, c,d \} \subseteq D_4$

A.B او B^{-1} پيدا کړې

ليما 3.7 : $(G,.)$ يو ګروپ او $\emptyset \neq U\subseteq G$. دالاندي افادي يوله بل سره معادل دي:

(1) U فرعی ګروپ د G دی

(2) $U.U \subseteq U , U^{-1}\subseteq U$

(3) $U. U^{-1}\subseteq U$

ثبوت:

$(1) \Rightarrow (2)$:

$u\,\epsilon U\,U \;\Rightarrow\; \exists\, u_1 , u_2\, \epsilon U \;, u =\; u_1 . u_2$

$\Rightarrow\; u =\; u_1 . u_2 \;\epsilon U$ [ځکه U فرعی گروپ دی]

$\Rightarrow\; U.U \;\subseteq U$

$a\epsilon U^{-1} \;\Rightarrow \exists\, b\, \epsilon U\,;\, a . b = e$

$\Rightarrow a = b^{-1}\, \epsilon U$ [$b\, \epsilon U$ ځکه]

$\Rightarrow\; U^{-1} \subseteq\; U$

(2) ⇐ (3):

$u\,\epsilon U\,U^{-1} \;\Rightarrow \exists\, u_1 \epsilon U \;\;\wedge\;\; u_2^{-1}\, \epsilon\, U^{-1}\,;\; u =\; u_1 . u_2^{-1}$

$\Rightarrow\; u_1\, \epsilon\, U \;\wedge\; u_2^{-1}\, \epsilon\, U$ [$U^{-1} \subseteq U$ ځکه]

$\Rightarrow\; u = u_1 . u_2^{-1}\, \epsilon U . U \;\subseteq U \;\;\Rightarrow\;\; U . U^{-1} \subseteq\; U$

(3) ⇐ **(1)** : دلته غواړو ثبوت کړو چې U د 3.1 قضيې (1) ، (2) او (3) خواص لري.

$a, b\epsilon U \;\Rightarrow\; e \;=\; b . b^{-1}\, \epsilon U . U^{-1} \subseteq U$

$\forall\, b\epsilon U\,, b^{-1} \;=\; e\, . b^{-1}\, \epsilon U . U^{-1} \subseteq U$

$a\, .\, b \;=\; a(b^{-1})^{-1}\, \epsilon U\, . U^{-1} \;\subseteq U$

ثبوت شو چې U يو فرعی گروپ د G دی .

تمرين 3.15:

(a) مونږپوهيږو چې $(\mathbb{Z}, +)$ يو گروپ دی. ثبوت کړی چې

$3\,\mathbb{Z} + 3\,\mathbb{Z} \;\subseteq 3\,\mathbb{Z} \;\;\wedge\;\; (3\,\mathbb{Z}\,)^{-1} \;\subseteq 3\,\mathbb{Z}$

(b) که مونږ $W := \{\, x \in \mathbb{R} \,|\, x > 0\,\}$ فرعی سيت په $(\mathbb{R}^*\,, .)$ گروپ کې ولرو . ثبوت کړی چې $W.W^{-1} \subseteq\; W$

(c) په استفاده د 3.7 ليما ثبوت کړی چې H={e,b,f,h} فرعی گروپ په D_4 کې دي.

نوټ 3.1 : (G , .) يو گروپ او U ، V دهغه فرعی گروپونه دي. په عمومي صورت د U او V Complex product (يعني U.V) يو فرعی گروپ د G د نه جوړوي . ددي هدف لپاره 3.5 مثال يوځل بيا مطالعه کوو. U او V فرعی گروپونه په لاندي ډول تعريف شوی دي.

$U := < f_2 > = \{id\,,\, f_2\}$

$V := < f_4 > = \{id\,,\, f_4\}$

$U.V = \{\, id\,,\, f_2\,, f_4\,,\, f_2 o f_4\,\}$

$= \{\, id\,,\, f_2\,,\, f_4\,,\, f_3\,\}$

$\Rightarrow\;\; \mathrm{ord(U.V)} = 4$

د Lagrange قضيي له مخې S_3 نه شي کولای فرعی کروپ ولري چې مرتبه (order) يې 4 وي. اويا داچې:

$f_3 \circ f_3 = f_1 \notin U.V$

لیما 3.8 : که $(G , .)$ یو گروپ او U ، V د هغه فرعی گروپونه وي . بیا:

$U.V$ یو فرعی گروپ (subgroup) د G دی . $\Leftarrow U.V = V.U$

ثبوت : د لیما 3.7 له مخې $V V^{-1} \subseteq V$ او $U U^{-1} \subseteq U$

$(UV) . (UV)^{-1} = UV.V^{-1} U^{-1} \subseteq U V U^{-1}$ [$V V^{-1} \subseteq V$ ځکه]

$= V U U^{-1} \subseteq V .U = U .V$

$\Rightarrow U . V$ subgroup (گروپ فرعی) [د 3.7 لیما مخې]

دپورتنی لیما څخه نتیجه اخلو چې Complex product د دوو فرعي کروپوهغه وخت یوفرعي گروپ جوړوي چې یو دهغوي نورمال وې .

قضیه 3.15 : $(G, .)$ ، $(G_1, *)$ دوه گروپونه چې $e\epsilon G$, $e_1\epsilon G_1$ دهغوي عینیت عناصراو $\varphi:G\to G_1$ یو G-Hom دی. بیا:

(a) $V \trianglelefteq G_1 \Rightarrow \varphi^{-1}(V) =\{ a\epsilon G \mid \varphi(a)\epsilon V \} \trianglelefteq G$

[یعني که V نورمال په G_1 کې وي ، بیا $\varphi^{-1}(V)$ نورمال په G کې دی]

(b) $\ker\varphi \trianglelefteq G$ [یعنې $\ker\varphi$ نورمال په G کې دی]

(c) که φ یو surjective هم وي ، بیا :

$N \trianglelefteq G \Rightarrow \varphi(N) \trianglelefteq G_1$

[یعني که N نورمال په G کې وي ، بیا $\varphi(N)$ نورمال په G_1 کې دی]

(a) **ثبوت :** د 3.3 قضیي له مخې $\varphi^{-1}(V)$ یو فرعی گروپ د G دی .

$x\epsilon \varphi^{-1}(V), a \epsilon G$

$\Rightarrow \varphi(x)\epsilon V , \varphi(a) \epsilon G_1 , \varphi(a^{-1}) \epsilon G_1$

$\Rightarrow \varphi(a.x.a^{-1}) = \varphi(a) * \varphi(x) * \varphi(a^{-1})\epsilon V$ [$V \trianglelefteq G_1$ ځکه]

$\Rightarrow a.x.a^{-1} \epsilon \varphi^{-1}(V)$

$\Rightarrow \varphi^{-1}(V)$ (normal) نورمال [د 3.6 لیما له مخی]

ثبوت (b) :

$a \epsilon G , x \epsilon ker\varphi \Rightarrow \varphi(x) = e_1$

$\Rightarrow \varphi(a . x . a^{-1}) = \varphi(a) * \varphi(x) * \varphi(a^{-1})$

$= \varphi(a) * e_1 * \varphi(a^{-1}) = \varphi(a.a^{-1})$

$= \varphi(e) = e_1$

$\Rightarrow a.x.a^{-1} \epsilon ker\varphi$

$\Rightarrow ker\varphi \trianglelefteq G$ [د 3.6 لیما له مخې]

ثبوت (c) **:** $\varphi(N)$ د 3.3 قضیه له مخې یو فرعی گروپ په G_1 کې دی .

$b\epsilon G_1 \Rightarrow \exists a\epsilon G ; \varphi(a) = b$ [surjective φ ځکه]

$\Rightarrow \forall x\epsilon N ; b * \varphi(x) * b^{-1} = \varphi(a) * \varphi(x) * \varphi(a^{-1})$

$= \varphi(a . x . a^{-1})$

N په G کې normal دی. پس 3.6 لیما له مخې $a\,.\,x\,.\,a^{-1}\epsilon N$
$a.x.a^{-1}\epsilon N \Rightarrow \quad b * \varphi(x) * b^{-1} = \varphi(a\,.\,x\,.\,a^{-1})\,\epsilon\varphi(N)$
په نتیجه کې د 3.6 لیما له مخې $\varphi(N)$ په G_1 کې Normal دی .

لیما 3.9 : $(G\,,+)$ یو ګروپ ، $e\in G$ عینیت عنصر او H یو فرعي ګروپ په G کې دی ، $x\in G$. بیا $x^{-1}\,.H\,.x = \{\, x^{-1}.h.x \mid h \in H\}$ یو فرعي ګروپ په G کی دی .

ثبوت :

$e = x^{-1}.e.x\in x^{-1}.H.x$
$a,b\in x^{-1}.H.x$
$\Rightarrow \exists\, h\,,k \in H\,; a = x^{-1}.h.x \;\wedge\; b = x^{-1}.k.x$
$\Rightarrow a.b = (x^{-1}.h.x)\,(x^{-1}.k.x)$
$= x^{-1}.h\,x\,.x^{-1}.k.x = x^{-1}.hkx$
$\Rightarrow a.b= x^{-1}\,.hkx \in x^{-1}.H.x$ [$h\,,k \in H$ ځکه]
$a = x^{-1}.h.x$
$\Rightarrow a^{-1} = (x^{-1}.(h.x))^{-1} = (hx)^{-1}.\,(x^{-1})^{-1} = x^{-1}.h^{-1}.x$
$\Rightarrow a^{-1} \in x^{-1}.H.x$ [$h \in H$ ځکه او $\boldsymbol{H}$ فرعي ګروپ]

په نتیجه کې $x^{-1}.H.x$ د 3.1 قضیې له مخې یو فرعي ګروپ د G دی .

لیما 3.10 : (G ,.) یو ګروپ ، e دهغه عینت عنصراو $a\in G$.
د $C_G(a)$ سیټ په لاندې ډول تعریف شوی دی:

$$C_G(a) = \{x \in G \mid x^{-1}.a.x = a\} = \{x \in G \mid a.x = x.a\}$$

$C_G(a)$ یو فرعي ګروپ د G دی او $a\in C_G(a)$.

ثبوت :- د ثبوت لپاره د 3.1 قضیې څخه استفاده کوو .

$e^{-1}\,.a\,.e = a \Rightarrow e \in C_G(a)$
$\Rightarrow x,y \in C_G(a) \Rightarrow x^{-1}\,a\,.x = a \;\wedge\; y^{-1}\,.a.y = a$
$\Rightarrow (xy)^{-1}\,a\,(xy) = y^{-1}\,.x^{-1}\,.a.x.y = y^{-1}\,a\,y = a$
$= y^{-1}.\,x^{-1}.\,x.\,a\,.y$ { $x \in C_G(a)$ ځکه]
$= y^{-1}.e.\,a\,.y = a$ { $y \in C_G(a)$ ځکه]
$\Rightarrow xy \in C_G(a)$
$x\in C_G(a) \Rightarrow x^{-1}\,a\,.x = a$
$a = x.x^{-1}\,a\,.x.x^{-1} = x.a..x^{-1} = (x^{-1})^{-1}\,.a\,.(x^{-1})$
$\Rightarrow x^{-1} \in C_G(a)$

ثبوت شو چې $C_G(a)$ یو فرعي ګروپ G کی دی. $C_G(a)$ د a د centralizer په نوم په G کی یادیږي

مثال: دلته د لیما 3.10 په استفادې سره غواړو C_{D_4} (c) فرعی گروپ پیداکړو

$C_{D_4}(c) = \{x \in D_4 \mid x^{-1}.c.x = c\}$

$e^{-1}.c.e = e.c.e = c \implies e \in C_{D_4}(c)$

$a^{-1}.c.a = c.c.a = b.a = c \implies a \in C_{D_4}(c)$

$b^{-1}.c.b = b.c.b = a.b = c \implies b \in C_{D_4}(c)$

$d^{-1}.c.d = d.c.d = f.d = a \implies d \notin C_{D_4}(c)$

همدارنگه f,g,h په C_{D_4} (c) شامل نه دي. یعنې $f,g,h \notin C_{D_4}(c)$.

په نتیجه کې $C_{D_4}(c) = \{e,a,b,c\}$

تمرین 3.16:

(1) په 1.6 مثال کی موولیدل چې (GL(2, ℝ),.) یو گروپ او عینیت عنصر یی واحد متریکس $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ دی.

H:= { A ∈ (GL(2, ℝ),.) | A diagonal (قطری) }

$M := \{ A \in GL(2, \mathbb{R}) \mid A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \}$

په 3.A مثال کی موولیدل چې H او M فرعی گروپونه په (GL(2, ℝ),.) کی دي کوم ددی فرعی گروپوڅخه نورمال په (GL(2, ℝ کـیدي.

(2) په (D₄,.) گروپ کې د H:= {e,h} فرعی گروپ لرو او $a \in D_4$. د 3.9 لیما څخه استفاده وکړئ اود { $U := \{a^{-1}.H.a\}$ فرعی گروپ پیدا کړی.

تمرین 3.17: د 3.10 لیما څخه استفاده وکړئ او بیا:

(a) د C_{D_4} (h) فرعی گروپ پیدا وکړئ

(b) د C_{S_3} (f_3) فرعی گروپ پیدا وکړئ

(c) د C_{Q_8} (g) فرعی گروپ پیدا وکړئ

تمرین 3.18: د $(Q_8,.)$ په گروپ کی مونږ لاندي سیتونه لرو :

H = { e,a,d,f} , H_1 = {e,a}

(1) ثبوت کړی چې H او H_1 فرعی گروپونه په Q_8 کی دي

(2) ord(a) په H_1 او ord(f) په H کی څودی

(3) ثبوت کړی چې H او H_1 دورانی دي

(4) دا لاندي ایندکسونه پیدا کړی:

$\text{ind}_{Q_8}(H_1)$, $\text{ind}_{Q_8}(H)$, $\text{ind}_H(H_1)$

تعریف 3.14: (.,G) یو گروپ او $e \in G$ عینیت عنصردی.

(a) $x \in G$ ته central او یا self-conjugate ویل کیږې که چیري $x.a = a.x$ (یعنې $x = a^{-1}.x.a$) وې

(b) سيت د ټولوعناصرو چې په G کې central وي د centere په نوم يادېږي او هغه په Z(G) ښيوو. يعني :

$Z(G):=\{x\in G \mid x=a^{-1}\,x\,.\,a \quad \forall\, a\in G\}$
$=\{ x\in G \mid x\,.\,a=a.\,x \quad \forall\, a\in G\}$

که G يو تبديلي (commutative) ګروپ وي. بيا Z(G) = G دی.

مثال 3.8 : په $(D_4,\ .\ )$ ګروپ کې {e,b} فرعي ګروپ centre د D_4 دي يعني : $Z(D_4)=\{e,b\}$. ځکه:

$\forall\, x\in D_4\ ;\ x^{-1}\,e\,.\,x=e \ \ \Rightarrow e\in Z(D_4)$
$a^{-1}\,b\,.\,a=c.\,b.\,a\ =a.\,a=b$
$c^{-1}\,b\,.\,c=a.\,b.\,c\ =c.\,c=b$
$d^{-1}\,b\,.\,d=d.\,b.\,d\ =g.\,d=b$

که همداډول ادامه ورکړل شي ، بيا ليدل کېږي چې f,g,h لپاره هم صدق کوي.
پس:

$\forall\, x\in D_4\,;\, b^{-1}\,.\,x\,.\,b=x\Rightarrow \mathrm{b}\in Z(D_4)$
$\Rightarrow\ Z(D_4)=\{e,b\}$

قضيه 3.16 : دهرګروپ (G , .) مرکز $Z(G)$ فرعي ګروپ دهغه دی.
ثبوت : ثبوت لپاره د 3.1 قضيي څخه استفاده کوو .

$\Rightarrow$ x,y$\in C_G(a)\ \ \forall\, a\in G \quad [3.10$ درليما $C_G(a)]$
$\Rightarrow\ x.\,y\,,x^{-1}\ \in C_G(a)\quad [$زيرا $C_G(a)$ يك ګروپ فرعي$]$
$\Rightarrow\ (x.y)^{-1}\,.\,a\,.\,(x.y)\ =a\ \ \wedge\ \ (x^{-1})^{-1}\,.a\,.\,x^{-1}=\ a\quad (\forall\, a\in G)$
$\Rightarrow\ \ a\,.\,(x.y)\ =(x.y)\ .\ a\ \ \wedge\ \ a\,.\,x^{-1}=(x^{-1})\,.\,a\quad (\forall\, a\in G$
$\Rightarrow\ \ (x.y)\,.\,a=a\,.\,(x.y)\ \ \wedge\ \ (x^{-1})\,.\,a=a\,.\,x^{-1}\quad (\forall\, a\in G)$
$\Rightarrow\ \ a^{-1}\,.\,(x.y)\,.\,a=\ (x.y)\ \ \wedge\ \ a^{-1}\,.(x^{-1})\,.\,a=\ x^{-1}\quad (\forall\, a\in G)$
$\Rightarrow x.\,y\,,x^{-1}\ \in Z(G)$

ثبوت شوچې Z(G) يو فرعي ګروپ د G دی .
نوټ: د هر ګروپ center نورمال هم دی
تعريف 3.15 : پريوګروپ (.,G) د (Aut(G په لاندي ډول تعريف شوی دی.

$\mathrm{Aut(G)}:=\{\ \mathrm{f{:}G}\rightarrow \mathrm{G}\mid \mathrm{f\ \ G-Autom}\ \}$

AutG نظرد تابع ترکيب (mapping composition) يو ګروپ دی چې عينيت عنصريي د Id تابع اومعکوس د (f $\in$Aut(G د $\boldsymbol{f^{-1}}$ تابع ده. مونږ هغه به (Aut(G), o) ښيوو .

قضيه 3. 17 : (G ,.) يو ګروپ دی. بيا :
(a) د G او (Auto(G ترمينځ يو ګروپ هومورفيزم φ موجود دی.

(b) ker(φ) په عین وخت کې Z(G) (یعني center) د G دی.

(a) ثبوت : د $g \in G$ لپاره φ تابع لاندي تعریفوم :

$$\varphi : G \longrightarrow Aut(G)$$
$$g \mapsto \varphi(g)$$

که اوس φ(g) په لاندي ډول تعریف شي:

$$\varphi(g): G \longrightarrow G$$
$$a \mapsto g\,.ag^{-1}$$

باید ثبوت شي چې $\boldsymbol{\varphi(g)}$ یو G-Autom دی .

$\boldsymbol{\varphi(g)}$ یو G-Hom :

$$a, b \in G\ , \varphi(g)(ab) = g\ a\ b\ g^{-1} = g.ag^{-1}g\ .\ bg^{-1}$$
$$= (gag^{-1}).(gbg^{-1})$$
$$= (\varphi(g)(a))\,.(\varphi(g)(b))$$
$$\Rightarrow \varphi(g) \quad G - Hom$$

$\boldsymbol{\varphi(g)}$ یو *injective* :

$$a \in \ker(\varphi(g)) \Rightarrow \varphi(g)(a) = e = g.a.g^{-1}$$
$$\Rightarrow g^{-1}.eg = a \Rightarrow a = e$$

خرنګه چې $\ker(\varphi(g)) = \{e\}$ دی ، پس د 2.3 قضیې له مخې $\varphi(g)$ یو injective دی .

$\boldsymbol{\varphi(g)}$ یو surjective :

$$y \in G\ ,\ x := g^{-1}y\,g$$
$$\varphi(g)(x) = \varphi(g)(g^{-1}y\,g) = g(g^{-1}y\,g)g^{-1} = e.y.e = y$$
$$\Rightarrow \varphi(g) \quad surjective$$

په نتیجه کې $\varphi(g) \in Aut\ G$

$\boldsymbol{\varphi}$ یو G-Hom :

$$g,h \in G \Rightarrow \forall\ a \in G\ ;\ \varphi(gh)(a) = (gh).a\,.(gh)^{-1}$$
$$= (gh).a.(h^{-1}g^{-1})$$
$$= g(h\,a\,h^{-1})g^{-1}$$
$$= \varphi(g)\,(hah^{-1})$$
$$= \varphi(g)(\varphi(h)(a))$$
$$= \varphi(g) \circ \varphi(h(a))$$
$$\Rightarrow \varphi(gh) = \varphi(g) \circ \varphi(h)$$

(b) ثبوت :

$$g \in \ker\varphi \Leftrightarrow \varphi(g) = id_G$$

$$\Leftrightarrow \ \varphi(g)(x) = id_G(x) = x \quad (\ \forall\, x \in G\ )$$
$$\Leftrightarrow gxg^{-1} = x \quad (\ \forall\, x \in G\ )$$
$$\Leftrightarrow gx = xg \quad \forall\, x \ \in G \qquad \Leftrightarrow g \in Z(G)$$

تعریف 3.16: (G ,.) یو ګروپ او N یو نورمال (Normal) فرعی ګروپ په G کې دی. set (مجموعه) د ټولو left-coset د N په G کې مونږ په G/N سره ښیو . یعني

$G/N \ := \ \{a.N \mid \ a\epsilon G\}$

قضیه 3.18 : (G ,.)یو ګروپ او N یو نورمال (Normal) فرعی ګروپ په G کې دی. بیا :

(a) G/N نظرلاندي دوه ګونی رابطي ته یو ګروپ دی .

$$\cdot : G/N \times G/N \longrightarrow G/N$$
$$(aN\,, bN) \ \longmapsto (aN)\,.\,(bN) \ = \ a.bN$$

(b) $|G\ /\ N| = [G:N]$

(c) که پر G او $(G/N\ ,.)$ باندي لاندې تابع تعریف شی :

$$\varphi: G \longrightarrow \ G/N$$
$$a \longmapsto a\ N$$

بیا :

(i) φ یوه G-Hom او surjective ده .

(ii) $ker\varphi = N$

(a) **ثبوت :-** څرنګه چې N یو نورمال (Normal) فرعی ګروپ په G کې دی ، پس بیا د $a\,, b\,\epsilon\, G$ لپاره صدق کوی:

$$aN = \ Na \quad \wedge \ \ bN = Nb$$

$$\Rightarrow (aN).(bN) \ = \ a(Nb)N \ = \ a(bN\,)N \ = \ a.b\ NN$$

د 3.7 لیما له مخې $NN \subseteq N$

$$n\epsilon N \ \Rightarrow \ n \ = \ e\,.\,n\,\epsilon\, NN \ \ \Rightarrow \ N \subseteq NN$$

په نتیجه کې N.N = N

$$(a\ N)\ (b\ N) \ = \ a\ b\ N\ N \ = \ a\ b\ N\,\epsilon\, G/N$$

پس (G/N ,.) یو الجبری جوړښت (ساختمان) لري. له بلي خوا

$$N(a\ N) = a\ NN = a\ N$$
$$\wedge$$
$$(a^{-1}N)(a\ N) = (a.a^{-1})N = e\ .\ N = N$$

له دي څخه نتیجه اخلو چې N عینیت عنصرد (G/N ,.) او $a^{-1}N$ معکوس د aN دی .

اتحادی خاصیت هم صدق کوي. ځکه: $a,b,c \epsilon G$

$$(a\,N).(b\,N\,.\,cN) = (a\,N)\,(b(Nc).N$$
$$= (aN)b(cN).N = \mathrm{(aN)(bc)N.N}$$
$$= (a\,N)(b\,c\,N) = a(N\,b\,c)N$$
$$= a.(b\,c\,NN)$$
$$= (a\,b\,c)N.N = a\,b\,c\,N$$

$$(aN\,.\,bN).cN = (a(Nb)N).cN = (abN.N).cN$$
$$= (abN).cN$$
$$= ab(Nc).N = ab(cN).N$$
$$= (abc)\,NN = abcN$$

ثبوت شو چې (G/N ,.) ګروپ دی چه د فکتوری ګروپ (factor group) په نوم یادیږي .

(b) **ثبوت :** د [G:N] تعریف له مخې صدق کوي.

(c) **ثبوت :**

(i) **ثبوت**

$$a,b \epsilon G\;;\; \varphi(ab) = a\,b\,N = \mathrm{abNN} = (aN)(bN)$$
$$= \varphi(a)\,.\,\varphi\,(b) \;\Rightarrow\; \varphi \quad G - Hom$$

φ : surjective φ (a) = aN دامعنی لري چې هر aN چپ کوست (Left-coset) یوانځور(تصویر) د a دی .

ثبوت (c) (ii):

$$a\epsilon\, ker\varphi \;\Rightarrow\; \varphi(a) = N \;\;\Lambda\;\; \varphi(a) = a.N$$
$$\Rightarrow\; N = a\,N \quad\Rightarrow\; a\,\epsilon\,N$$ [د 3.11 قضیې له مخې]
$$\Rightarrow\; ker\,\varphi\;\subseteq\; N$$

$$a\epsilon N \;\Rightarrow\; N = a\,N \;=\; \varphi(a) \Rightarrow\; a\,\epsilon\,\ker\varphi$$
$$\Rightarrow\; N \subseteq\; ker\,\varphi$$

په نتیجه کې $ker\,\varphi \;= N$

φ د canonical Epimorphysm په نوم یادیږي.

مثال 3.9 : مونږ ولیدل چې {e,b} د D_4 ګروپ center دی . یعني $Z(D_4)$={e,b} . څرنګه چې $Z(D_4)$ نورمال هم دی. پس کولای شو د D_4 فکتور

ګروپ (factor group) نظر $Z(D_4)$ د پورته قضیې له مخې $D_4/Z(D_4)$ پیدا کړو.
په دې معنې د $Z(D_4)$ ټول left-coset نظر کې نیسو .

$E:= Z(D_4) =\{e,b\}$

$A:= Z(D_4) . a = \{e,b\} .a = \{a , ba \} = \{a , c\}$

$\quad = Z(D_4) .c \ = \{a ,c \}$

$B:= Z(D_4) . d =\{e,b \} . d = \{d , bd\} = \{d ,g \}$

$\quad = Z(D_4) . g = \{ g,d\}$

$C:= Z(D_4) . f = \{e,b\} .f = \{f , bf \} = \{ f ,h\}$

$\quad = Z(D_4).h = \{h , f \}$

D_4 د left-coset شمیرنظر $Z(D_4)$ ته څلوردی. پس فکتور ګروپ

$D_4/ Z(D_4)=\{ E ,A , B , C \}$ او $E= Z(D_4)$ یې عینیت عنصردی.

$$\left|{}^{D_4}/_{Z(D_4)}\right| = [D_4 : Z(D_4)] = 4$$

دهغه کیلي جدول لاندي شکل لري:

	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

په جدول کې د مثال په ډول :

$A.B = Z(D_4).a \ \ Z(D_4) .d = (Z(D_4)).(Z(D_4))a.d$

$\quad = Z(D_4)\, a.d = Z(D_4) .f = C$

$A.A = Z(D_4).a.Z(D_4) .a = Z(D_4).Z(D_4).a.a$

$= Z(D_4) . b = Z(D_4) = E$ [د 3.11 قصيي له مخې]

تمرين 3.19:

(1) په 1.6 مثال کی موولیدل چې $(GL(2,\mathbb{R}), .)$ یو ګروپ دی.

(a)

$$S := \{ A \in M(2,\mathbb{R}) \mid A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \neq 0 \}$$

ثبوت کړی چې S یو فرعی ګروپ د $(GL(2,\mathbb{R}), .)$ دی

(b)

$H := \{ A \in (GL(2,\mathbb{R}), .) \mid$ A diagonal (قطری) $\}$

$M := \{ A \in GL(2,\mathbb{R}) \mid A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \}$

$N := \{ A \in (GL(2,\mathbb{R}), .) \mid \det A = 1 \}$

$S := \{ A \in M(2,\mathbb{R}) \mid A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \neq 0 \}$

په 3.A مثال کې ثبوت شو چې H ، M او N په $GL(2,\mathbb{R})$ کی فرعی ګروپونه دي. پیدا کړی چې د H، M،N ، S څخه کوم یو مرکز (center) د $GL(2,\mathbb{R})$ دی.

(2) مونږ د $N := \{e,a,b,c\}$ نورمال فرعی ګروپ په $(D_4,.)$ کې په نظر کې نیسو

(a) فکتوری ګروپ (Factor Group) $(D_4 /N ,.)$ پیداکړی.

(b) D_4/N ګروپ د کیلي جدول (cayley table) څه شکل لري.

تمرين 3.20: مونږ د $(Q_8,.)$ ګروپ په G سره ښیو

(a) ثبوت کړی چې $Z(G) = \{e,a\}$ دی

(b) د G ټول left-coset نظر $Z(G)$ ته پیدا کړی

(c) ثبوت کړی چې

$G = Z(G) \cup Z(G).b \cup Z(G). d \cup Z(G).g$

(d) $G /Z(G)$ پیداکړی اوپه کیلی جدول کې وښیی

ليما 3.11 : د نورمال فرعی ګروپو تقاطع بیاهم یو نورمال فرعی ګروپ دی .

ثبوت: مونږ یو ګروپ $(G,.)$ د e عینیت عنصرسره لرو.

$Ni(i\epsilon I, I = \{1,2, \dots ,n\})$ نورمال فرعی ګرروپونه په G کې دي او دهغوی تقاطع په N ښیو. یعنې

$$N := \bigcap_{i\epsilon I} N_i$$

غواړوثبوت کړوچي N نورمال په G کې دی . د لیما 3.2 له مخي N یوفرعی ګروپ د G دی. $a\epsilon G$

$$g \epsilon a N \Rightarrow \exists h \epsilon N ; g = a . h \Rightarrow a . h\epsilon a N_i \quad (\forall i \epsilon I)$$
$$\Rightarrow a . h = h . a \epsilon N_i . a \quad (\forall i \epsilon I)$$ [ځکه N_i نورمال دي]
$$\Rightarrow a. N \subseteq N. a$$

به همدی ډول کولای شوثبوت کړوچي $N . a \subseteq a N$ دی. په نتیجه کې $a. N = N. a$ او N نورمال په G دی .

قضیه 3.19 : (Theorem of group homomorphism)

(G,.) او (G₁ , ⋆) دوه ګروپه چې د عینیت عناصریي $e \in G$ ، $e_1 \in G_1$ او $\varphi: G \to G_1$ یو G-Hom دی. بیا دلاندي تابع یو G-Isom ده.

$$\varphi^- : G/ker\varphi \to \varphi(G)$$
$$a.\ker\varphi \to \varphi(a)$$

یعني فکتوری ګروپ $G/ker\varphi$ او $\varphi(G)$ ګروپ نظر φ^- ته له یوبل سره ایزومورف (Isomorph) دي. یعني $G/ker\varphi \cong \varphi(G)$

ثبوت :- د 3.15 قضیی له مخی $ker\varphi$ یو نورمال فرعي ګروپ دی.

اوهمدارنګه $\varphi(G)$ د 3.3 قضیی له مخی یوفرعي ګروپ دی . پس لهذا د φ^- تعریف درست دی. a,b∈ G

$$\varphi(a) = \varphi(b) \Rightarrow \varphi(a) = \varphi(b) * e_1 \Rightarrow \varphi(b)^{-1} * \varphi(a) = e_1$$
$$\Rightarrow \varphi(b)^{-1} * \varphi(a) = \varphi(b^{-1} . a) = e_1$$
$$\Rightarrow b^{-1}. a \in \ker\varphi$$
$$\Rightarrow a. \ker\varphi = b. ker\varphi$$ [د 3.11 قضیی له مخی]
$$\Rightarrow \varphi^- \quad injective$$

φ^- د تعریف له مخې $\varphi^-(G/ker\varphi) = \varphi(G)$ دی. پس φ^- یو surjective هم دی .

φ^- یو **G-Hom** :

د 3.15 قضیی په اساس مونږ پوهیږو چې $ker\varphi$ یونورمال فرعی ګروپ دی. پس لیکلی شو:

$$\varphi^-\big((a. ker\varphi). (b\ ker\varphi)\big)$$
$$\varphi^-\big((a. ker\varphi). (b\ ker\varphi)\big) = \varphi^-\big(ab\ (ker\varphi. ker\varphi)\big)$$
$$= \varphi^-(abker\varphi)$$

$= \varphi(a.b)$

$\varphi^{-}(aker\varphi) * \varphi^{-}(bker\varphi) = \varphi(a) * \varphi(b) = \varphi(a.b)$

$\Rightarrow \varphi^{-}$ G-Hom

په نتیجه کې φ^{-} يو G-Isom دی. يعني $G/\ker\varphi \cong \varphi(G)$

قضيه 3.20 : (theorem of group isomomorphism)

(G ,.) يو گروپ ، U يو فرعی گروپ او N فرعی نورمال گروپ په G کی دی.

بيا $U/\mathrm{U} \cap \mathrm{N}$ او UN/N له يو بل سره گروپ ايزومورف دي. يعنی:

$$UN/\mathrm{N} \cong U/\mathrm{U} \cap \mathrm{N}$$

ثبوت : د 3.18 قضيی له مخی دا لاندي تابع G-Hom ده:

$$\varphi: U \to G/N$$
$$a \mapsto a\,N$$

$\varphi(U) = \{\, \mathrm{uN} \mid \mathrm{u} \in \mathrm{U} \,\}$

$= \{\, \mathrm{uvN} \mid \mathrm{u} \in \mathrm{U}, \mathrm{v} \in \mathrm{N}\}$ [د 3.11 قضی له مخی]

$= UN/\mathrm{N}$ [د φ تعريف له مخی]

$\mathrm{u} \in \ker\varphi \Longrightarrow \mathrm{u} \in \mathrm{U} \wedge \mathrm{N} = \varphi(u) = uN$

$\Longrightarrow \mathrm{u} \in \mathrm{N}$ [د 3.11 قضی له مخی]

$\Longrightarrow \mathrm{u} \in \mathrm{U} \cap \mathrm{N}$

$\mathrm{u} \in \mathrm{U} \cap \mathrm{N} \Longrightarrow \mathrm{u} \in \mathrm{U} \wedge \mathrm{u} \in \mathrm{N} \Longrightarrow \varphi(u) = uN = N$

$\Longrightarrow \mathrm{u} \in \ker\varphi$

په نتيجه کی: $\ker\varphi = \mathrm{U} \cap \mathrm{N}$

د 3.19 قضی له مخی دالاندي تابع G-Isom ده:

$$\varphi^{-} : G/ker\varphi \to \varphi(G)$$
$$\mathrm{a.ker}\varphi \to \varphi(a)$$

په 3.11 ليما کی ثبوت شو چه UN فرعی گروپ په N ، G نورمال په UN او $\mathrm{U} \cap \mathrm{N}$ نو رمال په U کی دی. علاوه پردی $\varphi(U) = UN/\mathrm{N}$ او $\ker\varphi = \mathrm{U} \cap \mathrm{N}$ دي.

په نتيجه کی د 3.19 قضيه پرفرعی گروپ U باندی هم صدق کوی. يعنی دالاندي تابع يوه G-Isom ده

$$\varphi^{-} : U/\mathrm{U} \cap \mathrm{N} \to \varphi(U)$$
$$\mathrm{a.ker}\varphi \to \varphi(a)$$

څرنگه چه $\varphi(U) \cong U/\mathrm{U} \cap \mathrm{N}$ او $\varphi(U) = UN/\mathrm{N}$ دي. په نتيجه کی:

$$UN/N \cong U/U \cap N$$

نوټ:- مونږ.پوهیږو چې دهر $n \in \mathbb{N}$ لپاره د $n\,\mathbb{Z} = \{n \,.\, k \mid k \in \mathbb{Z}\}$ یو فرعي ګروپ د $(\mathbb{Z}\,, +)$ دی. څرنګه چې $(\mathbb{Z}\,, +)$ یو تبدیلي (commutative) ګروپ دی پس $n\,\mathbb{Z}$ یو نورمال فرعي ګروپ دی.

مثال 3.B: مونږ د $(\mathbb{R}^*, .)$ ګروپ په نظرکی نیسو.

$g: \mathbb{R}^* \longrightarrow \mathbb{R}^*$

$x \mapsto x^2$

(1) g یو G-Hom دی

حل:

$a, b \in \mathbb{R}^*$

$g(a.b) = (a.b)^2 = a^2.b^2 = g(a).g(b) \Rightarrow g$ G-Hom

(2) ker(g) یو نورمال فرعی ګروپ په $\mathbb{R}^*$ کی دی

حل:

$\ker(g) = \{ x \in \mathbb{R}^* \mid g(x) = 1 \} = \{ x \in \mathbb{R}^* \mid x^2 = 1 \} = \{ 1, -1 \}$

مونږ په 3.15 قضیه کی ولیدل چې kernel د یو G-Hom نورمال دی. پس پدي مثال کی ker(g) یو نورمال فرعی ګروپ په $\mathbb{R}^*$ کی دی.

$\mathbf{\mathbb{R}^*/\ker(g)}$: فکتور ګروپ په لاندي ډول دی:

$\mathbb{R}^*/\ker(g) = \{ x.\ker(g) \mid x \in \mathbb{R}^* \} = \{ x.\{ 1, -1 \} \mid x \in \mathbb{R}^* \}$

د هغه عینیت عنصر ker(g) دی

: $Z(\mathbb{R}^*)$

څرنګه چې $(\mathbb{R}^*, .)$ یو تبدیلی ګروپ دی، پس مرکز(center) یی $\mathbb{R}^*$ دی.

یعنې: $Z(\mathbb{R}^*) = \mathbb{R}^*$

:$g(\mathbb{R}^*) \cong \mathbb{R}^*/\ker(g)$

حل: φ په لاندي ډول تعریف شویده:

$\varphi : \mathbb{R}^*/\ker(g) \longrightarrow g(\mathbb{R}^*)$

$a.\ker(g) \longmapsto g(a)$

د حل لپاره د دولاندي طریقوڅخه کاراخلو

لمړی طریقه : څرنګه چې g یو G-Hom دی اوker(g) یو نورمال فرعی ګروپ په $\mathbb{R}^*$ کی دی ، پس φ د 3.19 قضیی له مخی یو isomorphism دی.

یعنې:

$\mathbb{R}^*/\ker(g) \cong g(\mathbb{R}^*)$

دویمه طریقه :

:φ injective

$a, b \in \mathbb{R}^*$, $\varphi(a.\ker(g)) = \varphi(b.\ker(g)) \Rightarrow g(a) = g(b)$

$\Rightarrow a^2 = b^2$

څرنګه چې b په $\mathbb{R}^*$ کی شامل دی، پس $b \neq 0$ دی.

$\Rightarrow \frac{1}{b^2}.a^2 = 1 \Rightarrow (\frac{1}{b}.a)^2 = 1 \Rightarrow g(\frac{1}{b}.a) = g(b^{-1}.a) = 1$

$\Rightarrow b^{-1}.a \in \ker(g) \Rightarrow a.\ker(g) = b.\ker(g)$ [د 3.11 قضیی له مخی]

$\Rightarrow$ φ injective

د **φ** تعریف له مخی ***surjective*** هم دی.

φ G-Hom:

$a,b \in \mathbb{R}^*$

$a.\ker(g)\ ,\ b.\ker(g) \in \mathbb{R}^*/\ker(g)$

$\varphi\ (\ (a.\ker(g)).\ (b.\ker(g)\ )\ = \varphi\ (ab.\ker(g)) = g(ab) = g(a).g(b)$

$\varphi\ (a.\ker(g))\ .\ \varphi\ (b.\ker(g)) = g(a)\ .\ g(b)$

$\Rightarrow g$ G-Hom

په نتیجه کی φ یو G-isom دی. یعنې: $g(\mathbb{R}^*) \cong \mathbb{R}^*/\ker(g)$

تمرین 3.21: $H=\{e,b,d,g\}$ یوفرعی سیت د $(D_4,.)$ په ګروپ کی دی

(1) ثبوت کړی چې H یو فرعی ګروپ د $(D_4,.)$ دی

(2) ایا H یو دورانی فرعی ګروپ دی

(3) ایا H یو تبدیلی فرعی ګروپ دی

(4) ثبوت کړی چې H یو نورمال فرعی ګروپ دی

(5) ټول left coset د $(D_4,.)$ ګروپ نظر H ته پیداکړی

(6) د D_4/H فکتورګروپ کوم عناصر لري

(7) D_4/H ګروپ په کیلی جدول کی وښیی

تمرین 3.22: $N=\{e,a\}$ یوفرعی سیت د $(Q_8,.)$ په ګروپ کی دی

(1) ثبوت کړی چې N یو فرعی ګروپ د $(Q_8,.)$ دی

(2) ایا N یو دورانی فرعی ګروپ دی

(3) ثبوت کړی چې N یو نورمال فرعی ګروپ دی

(4) ټول left coset د$(Q_8,.)$ ګروپ نظر N ته پیداکړی

(5) د Q_8/N فکتورګروپ کوم عناصر لري

(6) $Ord(Q_8/N)$ پیداکړی

(7) Q_8/N ګروپ په کیلی جدول کی وښیی

(8)

(a) د 3.18 قضیی څخه استفاده وکړی او یو φ ګروپ هومورفیزم د Q_8 او Q_8/N ترمینځ پیدا کړی

(b) ثبوت کړی چې φ یو surjective دہ، مګر injective نه ده

تعریف 3.17: $a \in \mathbb{Z}$ ، $0 \neq n \in \mathbb{N}$

$a+\ n\,\mathbb{Z} := \{a+nk\ \mid\ k\epsilon\,\mathbb{Z}\}$

$a + n\,\mathbb{Z}$ ته باقیمانده کلاس (residue class or congruence class) د a
نظرمودول(modulo) n ویل کیږي .که چیري دوه $a,b\epsilon\,\mathbb{Z}$ عدده په عین
باقیمانده کلاس کې یعنې $a+n\,\mathbb{Z} = b+n\,\mathbb{Z}$ وي، په دې صورت a
congrouent د b نظر n مودولو (modulo) په نوم یادیږي او
$a \equiv b$ (mod n) په ډول لیکل کیږي. په عمومي ډول کولای شو ووایوچې که
یوعدد a پر n تقسیم او r باقي پاتي شي ، هغه بیا په لاندې ډول لیکل کیږي:

$a \equiv r \ (\text{mod } n) \qquad 0 \le r < n$

د $a\epsilon\,\mathbb{Z}$ باقیمانده (پاتي) کلاس (residue class or congruence class)
نظر n مودولو (modulo) په $\bar{a}$ ښیو. یعنې :

$\bar{a} \ = a+ n\,\mathbb{Z} \ =\{\ a+n \mid k\epsilon\,\mathbb{Z}\ \}$

مثال:

8 mod 3 : 8 = 2.3 + 2 ⇒ 8 mod 3 = 2 ⇒ $8 \equiv 2$ (mod 3)
-8 mod 3 : - 8 = (-3).3 + 1 ⇒ - 8 mod 3 = 1 ⇒ $-8 \equiv 1$ (mod 3)
18 mod 5: 18 = 3.5 + 3 ⇒ 18 mod 5 = 3 ⇒ $18 \equiv 3$ (mod 5)
-18 mod 5: -18 = (-4).5 + 2 ⇒ -18 mod 5 = 2
⇒ $-18 \equiv 2$ (mod 5)
$14\equiv 2$ (mod 6) , $12\equiv 0$ (mod 6) , $13\equiv 3$ (mod 5) ,
$26\equiv 1$ (mod 5)

لیما 3.12 : د $a,b\ \in\ \mathbb{Z}$ او $0 \neq n\epsilon\mathbb{N}$ له پاره لاندې افادي یوله بل سره معادل دي

(1) $a \equiv b\ (mod\ n)$
(2) $a + n\,\mathbb{Z}\ =\ b + n\,\mathbb{Z}$
(3) $a - b\ \epsilon\ n\,\mathbb{Z}$
(4) که a او b پر n تقسیم شي مساوي باقیمانده لرې . یعنې

$a = q_1.n + r_1 \quad \wedge \quad b = q_2.n + r_2 \ \Longrightarrow\ r_1 \ = r_2$

ثبوت:

(1) ⟸ **(2)** : غواړو ثبوت کړوچې $a + n\,\mathbb{Z}\ =\ b + n\,\mathbb{Z}$

$h \in\ a + n\,\mathbb{Z} \Longrightarrow \exists\ k\,\epsilon\,\mathbb{Z}\,; h = a + k.n$

له بلې خوا:

$a \equiv b\ (mod\ n) \quad \Longrightarrow \exists\ q\,\epsilon\,\mathbb{Z}\,; a = \ q.n + b$

پس:

$h = a + k.n = q.n + b + k.n = b + (q{+}k).n\ \epsilon\ (\boldsymbol{b} + \boldsymbol{n}\mathbb{Z})$

$\Longrightarrow\ a + n\,\mathbb{Z}\ \subseteq\ b + n\,\mathbb{Z}$

په همدې ډول ثبوت کیدای شي چې: $b + n\,\mathbb{Z}\ \subseteq\ \ a + n\,\mathbb{Z}$

: (1) ⟸ (2)

$a+n\,\mathbb{Z}=b+n\,\mathbb{Z} \;\Longrightarrow \exists\; q_1,q_2 \in \mathbb{Z};\; a+q_1.n = b+q_2.n$

$\Longrightarrow a = (q_2-q_1).n+b$

$\Longrightarrow a \equiv b \;(mod\; n)$

: (3) ⟸ (2)

$h\in a+n\,\mathbb{Z} = b+n\,\mathbb{Z}$

$\Longrightarrow \exists\; q_1,q_2 \in \mathbb{Z};\; h = a+q_1.n = b+q_2.n$

$\Longrightarrow a-b = q_2.n - q_1.n = (q_2-q_1)n \in n\,\mathbb{Z}$

: (2) ⟸ (3)

$h \in a+n\,\mathbb{Z} \Longrightarrow \exists\; q \in \mathbb{Z};\; h = a+q.n$

له بلې خوا:

$a-b\in n\mathbb{Z}$

$\Longrightarrow \exists\; k \in \mathbb{Z};\; a-b = k.n \Longrightarrow a = b+k.n$

$\Longrightarrow h = a+q.n = b+k.n+q.n = b+(k+q).n \in b+n\mathbb{Z}$

$\Longrightarrow a+n\,\mathbb{Z} \subseteq b+n\,\mathbb{Z}$

په همدې ډول ثبوت کیدای شي چې: $b+n\,\mathbb{Z} \subseteq a+n\,\mathbb{Z}$. پس

$b+n\,\mathbb{Z} = a+n\,\mathbb{Z} \Longrightarrow (2)$

: (4) ⟸ (1)

$a \equiv b \;(mod\; n) \Longrightarrow \exists\; q \in \mathbb{Z};\; a = q.n+b$

له بلې خوا $b < n$ دی. پس $b = 0.n + b$ دی. لیدل کیږي چې a او b مساوی باقیمانده لري.په همدې ډول کولای شونوري افادي هم ثبوت کړو.

د $\mathbb{Z}$ ټولو باقیمانده کلاسو (residue class) سیت مودلو (modulo) n په $\mathbb{Z}\,/\,\boldsymbol{n}\,\mathbb{Z}$ اویا په $\mathbb{Z}_n$ ښودل کیږي. یعني :

$$\mathbb{Z}_n = \mathbb{Z}/n\,\mathbb{Z} = \{a+\; n\,\mathbb{Z}\;|a \in \mathbb{Z}\} = \{\bar{a}\;|a \in \mathbb{Z}\}$$

$\mathbb{Z}_n$ د n په شمیرمختلف باقیمانده کلاسي (residue class) لري. یعنې:

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, .\;.\;.\;., \overline{n-1}\},\; |\mathbb{Z}_n| = n$

په ځینوکتابوکې باقیمانده کلاسي (residue class) په لاندې ډول لیکل شوي دي:

$[a]_n = \{\, a\in\mathbb{Z} \mid a \equiv b \;(\text{mod } n) \,\}$

$\mathbb{Z}_n = \{ [0]_n, [1]_n, [2]_n, .\;.\;.\;.\;., [n\text{-}1]_n \}$

$[a] = \{\, a\in\mathbb{Z} \mid a \equiv b \;(\text{mod } n) \,\}$

$\mathbb{Z}_n = \{ [0], [1], [2], .\;.\;.\;.\;., [n\text{-}1] \}$

د مثال په ډول: $\mathbb{Z}_3 = \{ [0]_3, [1]_3, [2]_3 \}$

که د a باقیمانده کلاس (residue class) په $\bar{a}$ وښيو. په دې صورت د $\mathbb{Z}_3$
باقیمانده کلاسي لاندې عناصرلري :

$\bar{0} = \{. . . . , -12, -9 , -6 ,-3 ,0 , 3 ,6 , 9 ,12 , . . .\}$
$\bar{1} = \{. . . . ,-14, -11 , -8 ,-5 ,-2,1 , 4 ,7 , 10 ,13 , . . .\}$
$\bar{2} = \{. . . , -13, -10 , -7 ,-4 ,-1 , 5 ,8 , 11 ,14 , 17,. . .\}$

د مثال په ډول:

$12 = 4.3 + 0 \implies 12\epsilon\bar{0}$
$-14 = (-5).3 + 1 \implies -14\epsilon\bar{1}$
$-13 = (-5).3 + 2 \implies -13\epsilon\bar{2}$
$14 = 4.3 + 2 \implies 14\epsilon\bar{2}$

قضیه 3.21: $\mathbb{Z}_n$ نظر لاندې دوه ګوني رابطي ته يو دورانی ګروپ *(cyclic group)* دی .

$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$
$(a+ nZ, b+ n\mathbb{Z}) \longmapsto (a+ n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+ n\mathbb{Z}$

اويا $(\bar{a}, \bar{b}) \longmapsto \bar{a} + \bar{b} = \overline{a+b}$

د (3.18) قضيي له مخې $(\mathbb{Z}_n , +)$ يو ګروپ دی چې دهغه عينيت عنصر $\bar{0} = n\mathbb{Z}$ او $-\bar{a}= -a +n\mathbb{Z}$ معکوس د $\bar{a}=a+n\mathbb{Z}$ دی.
$(\mathbb{Z}_n , +)$ فکتوری ګروپ د باقیمانده کلاسوګروپ (residue class group) مودولو n په نوم ياديږي. اوس غواړوثبوت کړوچې د $\mathbb{Z}_n$ مولد (generator) عنصر $\bar{1} = 1 + n\mathbb{Z}\,\epsilon\mathbb{Z}_n$ دی.
د 3.7 ليما او 3.18 قضيی له مخې ليکلی شو:

$n\mathbb{Z} = n\mathbb{Z} + n\mathbb{Z} + ...+ n\mathbb{Z} = k.n\mathbb{Z}$ (k واري(دفعه))
$\mathbb{Z}_n = \{ k+ n\mathbb{Z} \mid k \in \mathbb{Z} \} = \{ k+k.n\mathbb{Z} \mid k \in \mathbb{Z} \}$]
$=\{ k.(1+ n\mathbb{Z}) \mid k \in \mathbb{Z} \}$
$= \{ k.\bar{1} \mid k \in \mathbb{Z} \} =< \bar{1} >$

په نتيجه کې $(\mathbb{Z}_n , +)$ يودورانی (cyclic) ګروپ دی او $ord(< \bar{1} >) = |\mathbb{Z}_n| = n$.

مثال 3.10 : مونږد $(\mathbb{Z}_6 , +)$ ګروپ په نظرکې نيسو. په دې ګروپ کې $ord(\mathbb{Z}_6) = |\mathbb{Z}_6| = 6$ او "+" دوه ګوني رابطه پر $\mathbb{Z}_6$ باندې د کيلي په جدول (cayley Table) ښيو .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

دهغه عینیت عنصر $6\mathbb{Z} = \bar{0}$ دی. د مثال په ډول $\mathbb{Z}$ 6+2- =$\bar{2}$- معکوس د $\mathbb{Z}$ 6+2 =$\bar{2}$ دی . ځکه :

$\bar{2} + (-\bar{2}) = (2 + 6\mathbb{Z}) + (-2 + 6\mathbb{Z}) = 2 + (-2) + 6\mathbb{Z} + 6\mathbb{Z}$
$= 0 + 6\mathbb{Z} + 6\mathbb{Z} = 6\mathbb{Z} = \bar{0}$

لیدل کیږي چې $(\mathbb{Z}_6 , +)$ یو تبدیلی ګروپ *(commutative)* دی .

نوټ : دمثال په ډول غواړم تشریح کړم چې څرنګه $\bar{4} = \bar{2}$ - کیږي

$\bar{4} + \bar{2} = \bar{6} = \bar{0} \Rightarrow \bar{4} = \bar{0} - \bar{2} = -\bar{2}$

د جدول دزیات تشریح لپاره څولاندي مثالونه :

$\bar{4} + \bar{5} = \bar{9} = \bar{6} + \bar{3} = \bar{0} + \bar{3} = \bar{3}$
$\bar{2} + \bar{5} = \bar{7} = \bar{6} + \bar{1} = \bar{0} + \bar{1} = \bar{1}$

څرنګه چې په جدول کې $\bar{0} = \bar{4} + \bar{2}$ او $\bar{0} = \bar{5} + \bar{1}$ دي. پس $\bar{2}$ او$\bar{4}$ معکوس دیوبل او همدارنګه $\bar{1}$او$\bar{5}$ معکوس دیوبل دي.

H:={ $\bar{0}, \bar{3}$} یو فرعی ګروپ دی. څرنګه چې $(\mathbb{Z}_6 , +)$ یو تبدیلی ګروپ دی. پس H نورمال هم دی . اوس غواړو د $(\mathbb{Z}_6)$ ټول کوسیت (coset) نظر H ته مطالعه کړو.

$U_0 = \bar{0} + H = \{\bar{0}, \bar{3}\}$
$U_1 = \bar{1} + H = \bar{1} + \{\bar{0}, \bar{3}\} = \{\bar{1}, \bar{4}\}$
$U_2 = \bar{2} + H = \bar{2} + \{\bar{0}, \bar{3}\} = \{\bar{2}, \bar{5}\}$
$\bar{3} + H = \bar{3} + \{\bar{0}, \bar{3}\} = \{\bar{3}, \bar{0}\} = H = U_0$
$\bar{4} + H = \bar{4} + \{\bar{0}, \bar{3}\} = \{\bar{4}, \bar{1}\} = \bar{1} + H = U_1$
$\bar{5} + H = \bar{5} + \{\bar{0}, \bar{3}\} = \{\bar{5}, \bar{2}\} = \bar{2} + H = U_2$

لیدل کیږي چې د $\mathbb{Z}_6$ د کوسیتو (coset) شمیرنظر H ته 3 دي. یعنې هغه U_0 ,U_1 ,U_2 دي . مونږ $G := (\mathbb{Z}_6 , +)$ وضع کو.

$G/H = \{ H, \bar{1} + H, \bar{2} + H \} = \{ U_0 , U_1 , U_2 \}$,
$ind(H) = 3$

مثال 3.11 : لاندې جدول ښيي چې $(\mathbb{Z}_7^*, .)$ يو ګروپ دی اوهغه لاندې باقيمانده کلاسي (residue class) لري.

$Z_7^* = \{[1], [2], [3], [4], [5], [6]\} \quad \wedge \quad |Z_7^*| = 6$

$[1] = 1 + 7\mathbb{Z}$

$[\mathbf{2}] = \mathbf{2} + \mathbf{7}\mathbb{Z}$

.

.

$[6] = 6 + 7\mathbb{Z}$

.	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

د

ليدل کيږي چې عينيت عنصريې [1] دی . تشريح لپاره دجدول ځومثالونه

$[4].[5] = [20] = [2].[7] + [6] = [2].[0] + [6] = [6]$
$[3].[6] = [18] = [2].[7] + [4] = [4]$

[2] او [4] معکوس ديوبل اود [6] پخپله [6] دي. ځکه:

$[4].[2] = [8] = [7] + [1] = [1]$

$[6].[6] = [36] = [5].[7] + 1 = [1]$

H:={[1] , [2], [4] } يو فرعی ګروپ د $(\mathbb{Z}_7^*, .)$ دی. ځکه :

(i) H نظر "." دوه ګوني رابطه الجبري جوړښت (ساختمان) لري.

$[1].[1] = [1] \in H$, $[1].[2] = [2] \in H$,
$[1].[4] = [4] \in H$, $[2].[4] = [8] = [1] \in H$,
$[4].[4] = [16] = [2] \in H$

(ii) $[1] \in H$

(iii) [4] او [2] معکوس ديوبل دي

پس د 3.1 قضيی له مخې H يوفرعي ګروپ په $\mathbb{Z}_7^*$ کې دی.

اوس غواړو د $\mathbb{Z}_7^*$ ټول کوسيت (cosets) نظر H ته پيدا کړو .

$[3].H = [3].\{[1], [2], [4]\} = \{[3], [6], [12]\}$
$= \{[3], [6], [5]\}$

$[5].H = [5].\{[1], [2], [4]\} = \{[5], [10], [20]\}$
$= \{[5], [3], [6]\}$

$[6].H = [6].\{[1],[2],[4]\} = \{[6],[12],[24]\}$
$=\{[6],[5],[3]\}$

په نتیجه کې:

$U := [3].H = [5].H = [6].H$
$ind(H) = 2\ ,\quad Z_7^*/H = \{H, U\}$

که د Lagrange قضیه تطبیق کړو

$|Z_7^*| = ord(H)\ .\ ind(H) \Rightarrow 6 = 3\ .\ ind(H)$

$$\Rightarrow ind(H) = \frac{6}{3} = 2$$

تمرین 3.20 : په $(Z_7^*, .)$ گروپ کې د $\bar{3}$ ، $\bar{4}$ او $\bar{6}$ مرتبه څوده . یعني $ord(\bar{3})$ ، $ord(\bar{4})$ او $ord(\bar{6})$ پیدا کړی

قضیه 3.22: که دالاندې دوه گوني رابطه (binary operation) پر $\mathbb{Z}_n$ باندې تعریف شي :

$$\cdot : \mathbb{Z}_n x \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
$$(a + n\mathbb{Z}, b + n\mathbb{Z}) \longmapsto (a + n\mathbb{Z}).(b + n\mathbb{Z}) := ab + n\mathbb{Z}$$

په مختصرډول کولای شوهغه $\bar{a}.\bar{b} = \overline{a.b}$ ولیکو، په دي شرط چې $\bar{a} := a + n\mathbb{Z}$ او $\bar{b} := b + n\mathbb{Z}$ وضع شي بیا :

(a) $(\mathbb{Z}_n, .)$ یو semigroup دی .

(b) $(\mathbb{Z}_n^*, .)$ یو گروپ دی، په دې شرط چې n یولمړنی (اولیه) عدد وي

ثبوت : باید ثبوت شی :

(i) $\bar{a} = \overline{a_1} \wedge \bar{b} = \overline{b_1} \Rightarrow \overline{a_1 b_1} = \overline{ab} \qquad (\bar{a}, \bar{b}, \overline{a_1}, \overline{b_1} \in \mathbb{Z}_n)$

(ii) $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n \Rightarrow \overline{ab} \in \mathbb{Z}_n$

(iii) $associativity$ (اتحادی)

(i) ثبوت:

$\bar{a} = \overline{a_1} \wedge \bar{b} = \overline{b_1} \Rightarrow a + n\mathbb{Z} = a_1 + n\mathbb{Z} \wedge b + n\mathbb{Z} = b_1 + n\mathbb{Z}$
$\Rightarrow a_1 - a \in n\mathbb{Z} \wedge b_1 - b \in n\mathbb{Z}$ [لیما له مخې 3.12]
$\Rightarrow a_1 - a \,|\, n \wedge b_1 - b \,|\, n$
$\Rightarrow \exists r, s \in \mathbb{Z}\ ;\ a_1 - a = nr \wedge b_1 - b = ns$
$\Rightarrow a_1 = a + nr \wedge b_1 = b + ns$
$\Rightarrow a_1 b_1 = (a + nr)(b + ns)$
$= ab + n(br + as + nrs)$

$$\Rightarrow \overline{a_1 b_1} = \overline{ab + n(br + as + nrs)} = \overline{ab} + \bar{0} = \overline{ab}$$

ثبوت (ii) :

$\bar{a} = a + n\mathbb{Z}\ , \bar{b} = b + n\mathbb{Z} \in \mathbb{Z}_{\ n}$
$\Rightarrow a, b \in \{0,1,2, \dots , n - 1\}$

لمړی حالت : که a.b < n وې. په دې صورت واضح ده چې $\overline{ab} \in \mathbb{Z}_n$

دویم حالت :که $a.b \geq n$ وې. په دې صورت:

$ab \geq n \Rightarrow \exists q, r \in \mathbb{N};$

$ab = nq + r \quad 0 \leq r < n \quad [division\ algorithm]$

$\Rightarrow \overline{ab} = \overline{nq + r} = \overline{nq} + \bar{r} = \bar{0} + \bar{r} = \bar{r}$

$\Rightarrow \overline{ab} \in \mathbb{Z}_n \qquad [0 \leq r \leq n]$

ثبوت: (iii)

$\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$
$\bar{a}.\left(\bar{b}.\bar{c}\right) = \bar{a}.\overline{bc} = \overline{a.b.c} = \overline{ab}.\bar{c} = \left(\bar{a}.\bar{b}\right).\bar{c}$

(b) ثبوت : مونږ فرضووچې n یو اولیه عدد دی .

$\mathbb{Z}_n^* \ = \{\ \bar{1}, \bar{2}.\bar{3}, \dots , \overline{n - 1})$
$\bar{a} \in \mathbb{Z}_n^*$
$\Rightarrow a \in \{1,2, \dots , n - 1\}$
$\Rightarrow \ \gcd(a, n) = 1$ [ځکه n عدد اولیه]
$\Rightarrow \exists r, s \in \mathbb{Z};\ ar + ns = 1 \quad [\ Euclidean\ algorithm \quad]$
$\Rightarrow \bar{1} = \overline{ra + ns} = \overline{ra} + \overline{ns} \ = \bar{r}.\bar{a} + \ \bar{0}.\bar{s} = \ \bar{r}.\bar{a}$

لیدل کیږې چې $\bar{r}$ معکوس د $\bar{a}$ دی .

په نتیجه کې $(\mathbb{Z}_n^*, .)$ یو ګروپي جوړښت (ساختمان) لري که چیرې n یو اولیه عدد وې. د $\mathbb{Z}_n^*$ عینیت عنصر $\bar{1} = 1 + n\mathbb{Z}$ دی .

مثال : $(\mathbb{Z}_4^*, .)$ په نظر کې نیسو. څرنګه چې 4 یو اولیه عدد نه دی ، پس باید د 3.21 قضیې له مخې $(\mathbb{Z}_4^*, .)$ ګروپ نه وی. څرنګه چې $\bar{2}.\bar{2} = \bar{0}$ او $\bar{0}$ په $(\mathbb{Z}_4^*, .)$ کې شامل نه دی اوله بلې خوا $\bar{2}$ معکوس نه لري.

.	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

مثال: غواړو $((\bar{2}\ .\ \bar{6})^3)^{-1}$ د $(\mathbb{Z}_7^*, .)$ په ګروپ کی پیدا کړو

حل:

$((\bar{2}\,.\,\bar{6})^3\,)^{-1} = ((\overline{12})^3\,)^{-1} = ((\bar{7} + \bar{5})^3)\,)^{-1} = ((\bar{0} + \bar{5})^3)\,)^{-1}$
$= ((\bar{5})^3\,)^{-1} = (\overline{25}.\bar{5})\,)^{-1} = ((\bar{3}.\bar{7} + 4).\bar{5}\,)^{-1}$
$= ((\bar{0} + \bar{4}\,).\bar{5}\,)^{-1}$
$=(\bar{4}.\bar{5}))^{-1} = (\overline{20})^{-1} = (\bar{6})^{-1} = \bar{6}$

اویا

$((\bar{2}\,.\,\bar{6})^3)\,)^{-1} = (\overline{12})^{-3} = (\bar{5})^{-3} = (\bar{5})^{-1}\,.\,(\bar{5})^{-1}\,.\,(\bar{5})^{-1} = \bar{3}\,.\,\bar{3}\,.\,\bar{3}$
$= \overline{27} = \overline{21} + \bar{6} = \bar{0} + \bar{6} = \bar{6}$

د $\bar{6}$ او $\bar{5}$ معکوس په لاندې شکل لاس ته راغلی دی :

$\bar{6}\,.\,\bar{6} = \overline{36} = \bar{5}\,.\,\bar{7} + \bar{1} = \bar{0} + \bar{1} = \bar{1} \Longrightarrow (\bar{6})^{-1} = \bar{6}$
$\bar{5}\,.\,\bar{3} = \overline{15} = \bar{2}\,.\,\bar{7} + \bar{1} = \bar{0} + \bar{1} = \bar{1} \Longrightarrow (\bar{5})^{-1} = \bar{3}$

تمرین 3.21:

(a) کوم یو د لاندې سیټوڅخه ګروپی جوړښت (ساختمان) نه لرې
$(\mathbb{Z}_6^*,.)$, $(\mathbb{Z}_{11}^*,.)$, $(\mathbb{Z}_4\,,+)$ او $(\mathbb{Z}_{11}\,,+)$

(b) $((\bar{4}\,.\,\bar{6})^2)\,)^{-1}$ ، $((\bar{2}\,.\,\bar{6})\,)^{-2}$ او $((\bar{2}\,.\,\bar{8})^2)\,)^{-2}$ په $(\mathbb{Z}_{13}^*\,,.)$ ګروپ کی پیدا کړی

قضیه 3.23 (Cayley theorem) : هرګروپ دهغه متناظرګروپ (symmetric group) دیو فرعی ګروپ ایزومورف (G-Isom) دی.
یعنی: که (G ,.) یو ګروپ او (S(G), ∘) دهغه متناظرګروپ وي، بیا یو فرعی ګروپ H په S(G) کې موجود دی، چه د G سره ایزومورف دی.
یعنی: $G \cong \mathrm{H}$

ثبوت: (G ,.) یوګروپ او e دعینیت عنصر دی . مونږد $a \in G$ لپاره د φ_a لاندې تابع په نظرکې نیسو:

$\varphi_a : G \longrightarrow G$
$x \longmapsto a.x$

φ_a یو bijective
څکه:

$x, y \in G$
$\varphi_a(x) = \varphi_a(y) \Rightarrow a.x = a.y \Rightarrow a^{-1}.a.x = a^{-1}.a.y$
$\Rightarrow e.x = e.y \quad \Rightarrow x = y \Rightarrow \varphi_a\ injective$

$y \in G$
$x := a^{-1}.y$
$\varphi_a(x) = \varphi_a(a^{-1}.y) = a.a^{-1}.y = e.y = y \Rightarrow \varphi_a\ sujective$

مونږ پر G سیټ دټولو پرموتیشن په S(G) ښیو. یعنی:

$S(G) := \{f : G \to G \mid f \quad bijective\,\}$

مونږپوهیږوچه S(G) د تابعو ترکیب له مخي یو ګروپ دی او عینیت عنصر یي د id تابع ده. اوس دالاندي تابع په نظرکي نیسو:

$$F : (G, .) \longrightarrow (S(G), \circ)$$
$$a \longmapsto \varphi_a$$

څرنګه چه φ_a بایجکتیف دی، پس تعریف د F هم درست دی.

F یو G-Hom :

د $g, h \in G$ لپاره باید ثبوت شي چه:

$$F(g.h) = F(g) \circ F(h)$$
$$F(gh) = \varphi_{gh}$$
$$\varphi_{gh}(x) = (gh).x = g.\varphi_h(x) = \varphi_g\left(\varphi_h(x)\right) = \left(\varphi_g \circ \varphi_h\right)(x)$$

$$\Rightarrow \; F(g.h) = F(g) \circ F(h) \Rightarrow F \;\; is \; G - Hom$$

$$F(g) = F(h) \Rightarrow \varphi_g = \varphi_h \Rightarrow \varphi_g(x) = \varphi_{h(x)} \;, \qquad \forall\, x \in G$$

$$\Rightarrow g.x = h.x \;\; , \forall\, x \in G \;\; \Rightarrow g.x.x^{-1} = h.x.x^{-1} \Rightarrow g.e = h.e$$
$$\Rightarrow g = h \;\Rightarrow F \;\; injective$$

مونږ image (تصویر) د G نظر F ته په H سره ښیو. یعنی:

$$H := F(G) \subseteq S(G)$$

نظر 2.4 قضیه ته H یو فرعی ګروپ د S(G) او $F : G \longrightarrow \mathrm{H}$ یو G-Isom دی. په نتیجه کي G ګروپ د S(G) یو فرعی ګروپ سره G-Isom دی.

مثال: (1.3 مثال کي) یوه دوه ګوني رابطه " *„ پر V={1,2,3,4} سیت بانه دي په کیلي جدول کي په لاندي ډول تعریف شویده:

*	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

په جدول کي لیدل کیږي چه عینیت عنصریي 1 دی. څرنګه چه:

$$2 * 2 = 3 * 3 = 4 * 4 = 1$$

پس دهرعنصر معکوس په خپله دی.

$(V,*)$ دپورتني جدول له مخي يو ګروپ دی او د Klein four-group په نوم يادېږي.
مونږدهغه متناظر ګروپ (symmetric group) په S(V) ښيو،چه عينيت عنصر يي د id ده. چهځرنګه $|V| = 4$ دی، پس:

$|S(V)| = 4\text{i} = 1.2.3.4 = 24$

يعنی S(V) ګروب 24 عناصرلري. د $a = 1,2,3,4$ لپاره لاندي تابع په نظرکي نيسو

$$\varphi_a : V \longrightarrow V$$
$$x \longmapsto a * x$$

$\varphi_1(V) = \{1*1, 1*2, 1*3\ , 1*4\} = \{1,2,3,4\}$

$\varphi_2(V) = \{2*1, 2*2, 2*3\ , 2*4\} = \{2,1,4,3\}$

$\varphi_3(V) = \{3*1, 3*2, 3*3\ , 3*4\} = \{3,4,1,2\}$

$\varphi_4(V) = \{4*1, 4*2, 4*3\ , 4*4\} = \{4,3,2,1\}$

اوس لاندي تابع په نظرنيسو:

$$F : (V,*) \longrightarrow (\ S(V),\circ)$$
$$a \longmapsto \varphi_a$$

$F(V) = \{\varphi_1(V), \varphi_2(V), \varphi_3(V), \varphi_4(V)\ \} \quad \wedge \quad |F(V)| = 4$

F(V) يو فرعی ګروپ د $(\ S(V),\circ)$ دی او $\varphi_1(V)$ يي دعينيت عنصردی.

$(\varphi_2 \circ \varphi_2)(V) = (\varphi_3 \circ \varphi_3)(V) = (\varphi_4 \circ \varphi_4)(V) = \varphi_1(V)$

پس دهر عنصر معکوس په خپله دی.

د کيلی قضيه له مخي V او F(V) يوبل سره ايزومورف دي. يعنی: $V \cong \text{F(V)}$

مثال: د $(\mathbb{Z}_3, +\ )$ګروپ کيلی جدول لاندي شکل لري:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

مونږ دهغه متناظر ګروپ (symmetric group) په $S(\mathbb{Z}_3)$ ښيو،چه عينيت عنصرد id ده. ځرنګه چه $|\mathbb{Z}_3| = 3$ دی، پس:

$|S(\mathbb{Z}_3)| = 3i = 1.2.3 = 6$

یعنی د S(V) گروب 6 عناصر لري. د $a = \bar{0}, \bar{1}, \bar{2}$ لپاره لاندي تابع په نظرکي نیسو:

$$\varphi_a : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$$
$$x \longmapsto a + x$$

$$\varphi_{\bar{0}}(\mathbb{Z}_3) = \{\bar{0} + \bar{0}, \bar{0} + \bar{1}, \bar{0} + \bar{2}\} = \{\bar{0}, \bar{1}, \bar{2}\}$$

$$\varphi_{\bar{1}}(\mathbb{Z}_3) = \{\bar{1} + \bar{0}, \bar{1} + \bar{1}, \bar{1} + \bar{2}\} = \{\bar{1}, \bar{2}, \bar{0}\}$$

$$\varphi_{\bar{2}}(\mathbb{Z}_3) = \{\bar{2} + \bar{0}, \bar{2} + \bar{1}, \bar{2} + \bar{2}\} = \{\bar{2}, \bar{0}, \bar{1}\}$$

اوس دالاندي تابع په نظرکي نیسو:

$$F : (\mathbb{Z}_3, +) \longrightarrow (S(\mathbb{Z}_3), \circ)$$
$$a \longmapsto \varphi_a$$

$$F(\mathbb{Z}_3) = (\varphi_{\bar{0}}(\mathbb{Z}_3), \varphi_{\bar{1}}(\mathbb{Z}_3), \varphi_{\bar{2}}(\mathbb{Z}_3)\} \quad \wedge \quad |F(\mathbb{Z}_3)| = 3$$

$F(\mathbb{Z}_3)$ یوفرعی گروپ د $(S(\mathbb{Z}_3), \circ)$ او $\varphi_{\bar{0}}(\mathbb{Z}_3)$ یي عینیت عنصردی.
$\varphi_{\bar{1}}(\mathbb{Z}_3)$ معکوس د $\varphi_{\bar{2}}(\mathbb{Z}_3)$ دی . ځکه:

$$(\varphi_{\bar{1}} \circ \varphi_{\bar{2}})(\mathbb{Z}_3) = \varphi_{\bar{1}}\{\bar{2}, \bar{0}, \bar{1}\} = \{\bar{1} + \bar{2}, \bar{1} + \bar{0}, \bar{1} + \bar{1}\}$$

$$= \{\bar{0}, \bar{1}, \bar{2}\} = \varphi_{\bar{0}}(\mathbb{Z}_3)$$

د کیلی قضیي له مخي $\mathbb{Z}_3$ او $F(\mathbb{Z}_3)$ یوبل سره ایزومورف دي.
یعنی: $\mathbb{Z}_3 \cong F(\mathbb{Z}_3)$

څلورم فصل

Direct product of groups

تعریف 4.1 : $(G_i, .)$ ګروپونه دي چې $e_i \in G_i$ $(i = 1,2,\dots,n)$ دهغوي عینیت عناصردي . که د G سیت په لاندې ډول تعریف شي

$$G := G_1 \times G_2 \times \dots \times G_n$$
$$= \{ (a_1, a_2, \dots, a_n) \mid a_i \in G_i \ (i = 1,2,3,\dots,n) \}$$

G د G_i (i= 1,2,3, . . . ,n) دګروپونو د cartesian product په نوم یادیږي اونظرلاندې دوه ګوني رابطي (Binary operation) ته ګروپ دی:

$$. : G \times G \to G$$
$$(a,b) \mapsto a . b$$
$$a = (a_1, a_2, a_3, \dots, a_n)$$
$$b = (b_1, b_2, b_3, \dots, b_n)$$
$$a . b = (a_1 . b_1, a_2 . b_2, \dots, a_n . b_n)$$

اتحادی خاصیت (associativity) :

$$a = (a_1, a_2, a_3, \dots, a_n), \quad b = (b_1, b_2, b_3, \dots, b_n),$$
$$c = (c_1, c_2, c_3, \dots, c_n)$$
$$(a . b). c$$
$$= [(a_1, a_2, \dots, a_n).(b_1, b_2, \dots, b_n)].(c_1, c_2, \dots, c_n)$$
$$= (a_1 . b_1, a_2 . b_2, \dots, a_n . b_n).(c_1, c_2, \dots, c_n)$$
$$= (a_1 b_1 c_1, a_2 b_2 c_2, \dots, a_n b_n c_n)$$
$$= (a_1, a_2, \dots, a_n).[(b_1, b_2, \dots, b_n).(c_1, c_2, \dots, c_n)]$$
$$= a.(b.c)$$

عینیت عنصر (identity): $e = (e_1, e_2, e_3, \dots, e_n)$

معکوس(inverse) :

د $a = (a_1, a_2, \dots, a_n)$ معکوس $a^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$ دی. ځکه :

$$a . a^{-1} = (a_1, a_2, \dots, a_n).(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$$
$$= (a_1 . a_1^{-1}, a_2 . a_2^{-1}, \dots, a_n . a_n^{-1})$$
$$= (e_1, e_2, \dots, e_n) = e$$

(G,.) د External direct product ګروپ په نوم یادیږي.

مثال 4.1 : $G_2 = G_1 = \{1, -1\}$. پوهیږوچې $(G_1, .)$ او $(G_2, .)$ نظر ضرب ته ګروپې جوړښت (ساختمان) لري چې 1 دهغه عینیت عنصردی.

$G = G_1 \times G_2 = \{1,-1\} x \{1,-1\}$
$= \{(1,1), (1,-1), (-1,1), (-1,-1)\}$

د (G,.) گروپ کيلی جدول (cayley table) په لاندې ډول دی .

.	(1 ,1)	(1 ,-1)	(-1 ,1)	(-1 ,-1)
(1 ,1)	(1 ,1)	(1 ,-1)	(-1 ,1)	(-1 ,-1)
(1 ,-1)	(1 ,-1)	(1 ,1)	(-1 ,-1)	(-1 ,1)
(-1 ,1)	(-1 ,1)	(-1 ,-1)	(1 ,1)	(1 ,-1)
(-1 ,-1)	(-1 ,-1)	(- 1 ,1)	(1 ,-1)	(1 ,1)

(G,.) گروپ يو external direct product (ext – dir – prod) د G_1 او G_2 دي چې دهغه عينيت عنصر e = (1,1) او ordG = 4 دی .
په عمومي ډول که مونږ A , B او C دري گروپونه ولرو چې ord A= 3 , ordB=5 او ordC=6 وي. که G = AxBxC وي په دې صورت ordG = 3.5.6 = 90 کيږي. يعنې د G د عناصروشمير 90 دی .

مثال: دلته مونږ د $(\mathbb{R},+)$ او $(\mathbb{R}^*,.)$ گروپونه په نظرکې نيسو. که $G:= \mathbb{R}^* \times \mathbb{R}$ وي، بيا G نظرلاندې دوه گوني رابطې له مخې يو (ext – dir – prod) گروپ د $\mathbb{R}$ او $\mathbb{R}^*$ دی چې عينيت عنصريي (1,0) دی.

$* : G \times G \longrightarrow G$
$(a,b) \longmapsto a*b$

د $a = (a_1,a_2)$, $b = (b_1, b_2) \in G$ حاصل په لاندې ډول دی:

$a*b = (a_1,a_2) * (b_1, b_2) = (a_1 . b_1, a_2+ b_2)$

$a^{-1} = (\frac{1}{a_1}, - a_2)$, $b^{-1} = (\frac{1}{b_1}, - b_2)$

د مثال په ډول $b = (2,4), a = (3,5)$

$a*b = (3, 5) * (2, 4) = (3.2, 5+4) = (6,9)$

$a^{-1}= (\frac{1}{3}, -5)$, $b^{-1}= (\frac{1}{2}, -4)$

ځکه:

$a * a^{-1} = (3,5) * (\frac{1}{3}, -5)= (3.\frac{1}{3},5 -5)=(1,0)$

$b * b^{-1} = (2,4) * (\frac{1}{2}, -4)= (2.\frac{1}{2},4 -4)=(1,0)$

تمرين 4.1 :

(1) مونږ د $A^{(4)}$, $A^{(2,2)}$ و D_4 گروپونه په نظرکې نيسو. که $G:= D_4 \times A^{(2,2)} \times A^{(4)}$ وي

(a) د G عينيت عنصر (identity) کوم دی

(b) په G کې د (c,b_4,a_3) معکوس (inverse) پیدا کړئ
(c) G د عناصرو شمیرڅو دي. یعني $ordG = |G|$ پیدا کړئ
(d) په G کې ځلورهغه عنصره پیدا کړئ چې معکوس یې په خپله وي
(2) مونږپوهیږو چې $(\mathbb{Z}_3, +)$ یو ګروپ دی . که $G:= \mathbb{Z}_3 \times \mathbb{Z}_3$ وي
(a) د G عینیت عنصر (identity) کوم دی
(b) په G کې د $(\overline{1}, \overline{2})$ معکوس (inverse) پیدا کړئ
(c) G د عناصرو شمیرڅو دي. یعني $ordG = |G|$ پیدا کړئ
(d) د $(G,.)$ ګروپ په Cayley جدول کې وښیی
(3) مونږ د $(\mathbb{Z}_{11}, +)$ او $(\mathbb{Z}^*_{11}, .)$ ګروپونه لرو.

$G:= \mathbb{Z}^*_{11} \times \mathbb{Z}_{11}$

(a) د G عینیت عنصر (identity) کوم دی
(b)

$\bar{x} = (\overline{5}, \overline{6})$, $\bar{y} = (\overline{4}, \overline{9}) \in G$

$\bar{x}.\bar{y}$ پیداکړئ
(c) G د عناصرو شمیرڅو دي. یعني $ordG = |G|$ پیدا کړئ

تمرین 4. 2 :

$G_1 = \{1, -1 \subseteq \mathbb{R}, G_2 = \{1, -1, i, -i\} \subseteq \mathbb{C} \quad , G = G_1 X G_2$

پوهیږوچې $(G_1, .)$ او $(G_1, .)$ ګروپونه دي. البته دوه ګوني رابطه دلته ضرب "." ده . د $(G, *)$ ګروپ ext- dir – prod دهغوې دی. د $(G, *)$ کیلی (Cayley) جدول څه ډول دی .

تمرین 4.3 : پوهیږوچې $(\mathbb{Z}_2, +)$ یو ګروپ دی. که $G:= \mathbb{Z}_2 \times \mathbb{Z}_2$ وې،
بیا په Cayley جدول کې وښیې چې $(G, .)$ یو ګروپ دی.

لیما 4.1: $(G ,.)$ یو ګروپ چې $e\in G$ یې عینیت عنصراو H_2 , H_1 د لاندې خواصوسره د هغه فرعی ګروپونه دي.

(I) $H_1 \cap H_2 = \{e\}$
(ii) $H_1 . H_2 = G$
(iii) $x .y = y .x \quad (\forall x\in H_1 \wedge \forall y\in H_2)$

بیا دالاندې تابع G- isom ده :

$$\varphi: H_1 \times H_2 \longrightarrow G$$
$$(x , y) \longmapsto x . y$$

ثبوت :

$\boldsymbol{\varphi}$ **G − Hom**:

$x = (x_1, x_2), y = (y_1, y_2) \in H_1 \times H_2$

$\varphi(x.y) = \varphi((x_1, x_2).(y_1, y_2)) = \varphi(x_1.y_1, x_2.y_2)$

$= x_1 y_1 . x_2 y_2$

$\varphi(x) = \varphi(x_1, x_2) = x_1.x_2 \wedge \varphi(y) = \varphi(y_1, y_2) = y_1.y_2$

$\varphi(x).\varphi(y) = x_1 x_2 . y_1 y_2$

$= x_1 y_1 . x_2 y_2$ [د (iii) له مخې]

$= \varphi(x.y)$

$\Rightarrow \varphi$ G − Hom

$\boldsymbol{\varphi}$ **surjective** :

$g \in G \Rightarrow \exists h_1 \in H_1 \wedge h_2 \in H_2$;

$g = h_1 . h_2$ [$H_1.H_1 = G$ ځکه]

$\Rightarrow \varphi(h_1, h_2) = h_1.h_2 = g$

$\Rightarrow \varphi$ surjective

$\boldsymbol{\varphi}$ **injective** :

$(x, y) \in \ker\varphi \Rightarrow \varphi(x, y) = e = x.y \Rightarrow x = y^{-1}$

$\Rightarrow x \in H_1 \wedge y^{-1} \in H_2$ [$y^{-1}, y \in H_2$ ځکه]

$\Rightarrow x, y^{-1} \in H_1 \cap H_2$

$\Rightarrow x = e \wedge y^{-1} = e$ [$H_1 \cap H_2 = e$ ځکه]

$\Rightarrow (x, y) = (e, e)$

$\Rightarrow \varphi$ injective [د 2.3 قضیې له مخې]

په نتیجه کې ثبوت شوچې φ یو G- isom دی .

مثال 4.2 : مونږ د A او B دوه دورانی ګروپونه لرو چې $e_1 \in A$ او $e_2 \in B$ دهغوې عینیت عناصردي .

$< a > = A = \{e_1, a\} \wedge a^2 = e_1$

$< b > = B = \{e_2, b, b^2\} \wedge b^3 = e_2$

$G := A \times B$

$= \{(e_1, e_2), (e_1, b), (e_1, b^2), (a, e_2). (a, b), (a, b^2)$

G نظرلاندې دوه ګونې رابطې ته یو ext-dir – prod ګروپ د A او B دی

$\cdot : G x G \longrightarrow G$

$(x,y) \longmapsto x.y$

دلته د $x = (x_1,x_2)$, $y = (y_1,y_2)$ لپاره

$x.y = ((x_1,x_2) . (y_1,y_2) = (x_1. y_1, x_2.y_2)$

$e=(e_1 , e_2)$ د هغه عینیت عنصر او (x^{-1},y^{-1}) معکوس د (x,y) دی . د مثال په ډول غواړو معکوس (a,b^2) پیداکړو

$$a.a = a^2 = e_1 \Rightarrow a^{-1} = a$$

$$b^2.b = b^3 = e_2 \Rightarrow (b^2)^{-1}.b^2.b = (b^2)^{-1}.e_2$$

$$\Rightarrow e_2 .b = b = (b^2)^{-1}$$

لیدل کیږي چې a^{-1} معکوس د a او b معکوس د b^2 دی .

$$A':= \{(x, e_2) \mid x \in A\} =\{(e_1 , e_2), (a, e_2)\}$$

$$B' := \{(e_1 , x) \mid x \in B\} = \{(e_1 , e_2), (e_1 , b), (e_1 , b^2)\}$$

A´ او B´ نورمال فرعی ګروپونه په G کې دي .

په آسانی ښودل کیدې شي چې A´ او B´ فرعی ګروپونه په G کې دي . اوس غواړو ثبوت کړو چې A´ او B´ نورمال دي.

د 3.6 لیما له مخې باید ثبوت شی :

$$\forall x =(x_1 , x_2) \in G;\ x B' x^{-1} \subseteq B'$$

$$y = (y_1 , y_2) \in x.B'x^{-1}$$

$$\Rightarrow \exists b' = (b_1 , b_2) \in B' ; y = x b'x^{-1}$$

$$= (x_1 , x_2).(b_1 , b_2).(x_1^{-1} , x_2^{-1})$$

$$b' = (b_1, b_2) \in B'$$

$\Rightarrow b_1 = e_1 \in A \wedge b_2 \in B'$ [تعریف له مخې]

$$y = (y_1 , y_2) = x b'x^{-1} = (x_1 b_1 x_1^{-1}, x_2 b_2 x_2^{-1})$$

$$= (x_1 e_1 x_1^{-1}, x_2 b_2 x_2^{-1})$$

$$= (e_1 , x_2 b_2 x_2^{-1})$$

له بلې خوا

$$X_2 , b_2 \in B \Rightarrow x_2 .b_2 \in B$$

$\Rightarrow x_2 .b_2.x_2^{-1} \in B$ [ځکه B یو فرعی ګروپ دی]

$$\Rightarrow y = (e_1 , x_2 b_2 x_2^{-1}) \in B' \Rightarrow B'\ normal$$

په همدې ډول کولای ثبوت کړوچې A´ هم نورمال په G کې دی .

تعریف 4.2 : (. , G) یو ګروپ او $e\in G$ عینیت (identity) عنصر دی .

$N_1, N_2, . . . , N_n$ نورمال فرعی ګروپونه په G کې دلاندي خواصوسره دي

(i) $G = N_1.N_2. . . . .N_n$

$$= \{(a_1. . . . .a_n) \mid a_i \in N_i\ (i = 1,2, \dots , n)\}$$

(ii) $N_k \cap (N_1.N_2 . . . . .N_{k-1} .N_{k+1}\dots N_n)$

$$= \{e\} \quad (k = 1,2,3, \dots , n)$$

G ګروپ ته internal direct product (ent-dir-prod) د N_i

ویل کیږي (i= 1 ,2 ,3 , . . . , n)
که G یو ent- dir – prod د N_i (i= 1 ,2 ,3 , . . . , n) وي. بیا هغه په لا ندې شکل لیکل کیږي

$$G = N_1 \otimes N_2 \otimes \ldots . \otimes N_n$$

مثال 4.3 : د $(A^{(2,2)}, \odot)$ ګروپ کې لاندې فرعي ګروپونه لري :

$$< b_2 > = \{b_1 , b_2\} \quad , < b_3 > = \{b_1 , b_3\}$$

څرنګه چې $A^{(2,2)}$ یو تبدیلی ګروپ دی. پس $<b_2>$ او $<b_3>$ نورمال دي

$$< b_2 > . < b_3 > = \{b_1 , b_2\}. \{b_1 , b_3\}$$
$$= \{b_1, b_3, b_2 , b_4\} = A^{(2,2)}$$
$$< b_2 > \cap < b_3 > = \{b_1 , b_2\} \cap \{b_1 , b_3\} = \{b_1\}$$

په نتیجه کې $A^{(2,2)}$ یو ent- dir –prod د $< b_2 >$ او $< b_3 >$ دی .
یعنې $A^{(2,2)} = < b_2 > \otimes < b_3 >$

مثال 4.4 : په $(\mathbb{Z}_6 , +)$ ګروپ کې لاندې فرعی ګروپونه لرو :

$$<\bar{2} > = \{\bar{0} , \bar{2} , \bar{4}\} \quad , < \bar{3} > = \{\bar{0}, \bar{3}\}$$

څرنګه چې $\mathbb{Z}_6$ تبدیلی (commutative) ګروپ دی. پس $<\bar{2}>$ او $<\bar{3}>$ نورمال دي

$$<\bar{2} > + < \bar{3} > = \{\bar{0} , \bar{2} , \bar{4}\} + \{\bar{0}, \bar{3}\} = \{\bar{0}, \bar{2}, \bar{4}, \bar{3}, \bar{5}, \bar{1}\} = \mathbb{Z}_6$$
$$<\bar{2} > \cap < \bar{3} > = \{\bar{0}\}$$

پس $\mathbb{Z}_6 =< \bar{2} > \otimes < \bar{3} >$ دی. یعنې $\mathbb{Z}_6$ یو ent-dir-prod د $<\bar{2}>$ او $<\bar{3}>$ دی .

مثال 4.5 : $(\mathbb{Z}_8^*,.)$ ګروپ کیدی نشې . ځکه 8 یولمړنی (اولیه) عدد نه دی. د مثال په ډول

$$\bar{4} \in \mathbb{Z}_8^* \;,\; \bar{4}.\bar{4} = \overline{16} = \bar{0} \notin \mathbb{Z}_8^*$$

مونږ د $(\mathbb{Z}_8^*,.)$ ټول معکوس لرونکې (پذیر) عناصر په $\mathbb{Z}_8^x$ سره ښیو :

$$\mathbb{Z}_8^x = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$

$(\mathbb{Z}_8^x,.)$ یو ګروپ دی اود هغه کیلی جدول لاندې شکل لري:

.	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

$<\bar{3}>$ او $<\bar{5}>$ د $(\mathbb{Z}_8^x,.)$ فرعی گروپونه دي .اوس به وښيوچې $\mathbb{Z}_8^x$ يو ent-dir-prod د $<\bar{3}>$ او $<\bar{5}>$ دی

$<\bar{3}> = \{\bar{1},\bar{3}\}$, $<\bar{5}> = \{\bar{1},\bar{5}\}$
$<\bar{3}>.<\bar{5}> = \{\bar{1},\bar{3}\}.\{\bar{1},\bar{5}\} = \{\bar{1},\bar{3},\bar{5},\bar{7}> = \mathbb{Z}_8^x$
$<\bar{3}> \cap <\bar{5}> = \bar{1}$

په نتيجه کې $\mathbb{Z}_8^x = <\bar{3}> \otimes <\bar{5}>$ دی

تمرين 4.5 : $(\mathbb{Z}_8^x,.)$ گروپ په نظر کې نيسو.ثبوت کړی چې $\mathbb{Z}_8^x = <\bar{5}> \otimes <\bar{7}>$ او $\mathbb{Z}_8^x = <\bar{3}> \otimes <\bar{7}>$ کيږي

تمرين 4.6: د $(\mathbb{Z}_6,.)$ څخه $\mathbb{Z}_6^x$ اود $(\mathbb{Z}_{10},.)$ د $\mathbb{Z}_{10}^x$ گروپ پيدا کړی

تمرين 4.7 : د (Q,.) گروپ < I > او < k > فرعي گروپونه لري

(a) پورتنې فرعی گروپونه کوم عناصرلرې او د هغوې مرتبه (order) پيداکړی

(b) ايا د Q گروپ يو ent-dir-prod د < I > او < k > دی. يعني

$$Q = < I > \otimes < K >$$

ليما 4.2: مونږ $r_{1,} r_{2,} \dots, r_n$ طبعی اعداد چه خلاف دصفراوپريوبل باندي قابل د تقسم نه دي، لرو. يعنی:

$$\gcd(r_{i,} r_j) = 1 \quad (i,j = 1,2,\dots,n \ \wedge \ i \neq j)$$

بيا د هر $k \in \mathbb{N}$ لپاره لاندي تابع يو R-Isom (رينگ ايزومورف) ده:

$$\psi: \mathbb{Z}_{r_1.r_2\dots r_n} \longrightarrow \mathbb{Z}_{r_1} x\, \mathbb{Z}_{r_2} x \dots x\, \mathbb{Z}_{r_n}$$
$$k + r_1.r_2 \dots r_n\mathbb{Z} \longmapsto (k + r_1\mathbb{Z}, k + r_2\mathbb{Z}, \dots, k + r_n\mathbb{Z})$$

ثبوت:

$r := r_1.r_2 \dots r_n$
$\boldsymbol{\psi\ injective}$:

$k + r\mathbb{Z}, m + r\mathbb{Z} \in \mathbb{Z}_r$

$k + r\mathbb{Z} = m + r\mathbb{Z} \Leftrightarrow k - m \in r\mathbb{Z}$ [د 3.12 ليما له مخی]

$\Leftrightarrow r \mid k - m \Leftrightarrow r_i \mid k - m \quad [i = 1,2,\dots,n]$

$\Leftrightarrow k + r_i\mathbb{Z} = m + r_i\mathbb{Z} \quad [i = 1,2,\dots,n]$

$\Leftrightarrow \psi(k + r\mathbb{Z}) = \psi(m + r\mathbb{Z})$

$\Leftrightarrow \psi$ *injective*

ψ surjective:

$|\mathbb{Z}_r| = r = \prod_{i=1}^{n} |\mathbb{Z}_{r_i}| = |\mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \dots \times \mathbb{Z}_{r_n}|$

ځرنګه چه دومين (domain) اوکودومين (codomain) سيتونه متناهی او د عناصرو شميريي سره مساوی دی، پس د 0.1 قضيي له مخي د ψ تابع سورجيکتيف ده .

له بلي خوا ψ د تعريف له مخي يو R-Hom (د قضيي 3.18 د ثبوت په نظرکي نيولو سره) ده . په نتيجه کي ψ يوR-Isom دی.

مثال:

$r_1 = 2, r_2 = 3, r = r_1.r_2 = 2.3 = 6$

$\psi: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$

$k + 6\mathbb{Z} \longmapsto (k + 2\mathbb{Z}, k + 3\mathbb{Z})$

4.2 ليماله مخي د ψ تابع يو R-Isom ده. مګربياهم غواړوهغه پدي مثال کي ثبوت کړو

$k + 6\mathbb{Z}, m + 6\mathbb{Z} \in \mathbb{Z}_6$

$\psi\big((k + 6\mathbb{Z}) + (m + 6\mathbb{Z})\big) = \psi((k + m) + 6\mathbb{Z})$

$= ((k + m) + 2\mathbb{Z}, (k + m) + 3\mathbb{Z})$

$= ((k + 2\mathbb{Z}) + (m + 2\mathbb{Z}), (k + 3\mathbb{Z}) + (m + 3\mathbb{Z}))$

$= (k + 2\mathbb{Z}, k + 3\mathbb{Z}) + (m + 2\mathbb{Z}, m + 3\mathbb{Z})$

$= \psi\big((k + 6\mathbb{Z}) + \psi(m + 6\mathbb{Z})\big)$

$\psi\big((k + 6\mathbb{Z}).(m + 6\mathbb{Z})\big)$

$= \psi(k.m + 6\mathbb{Z}) = (km + 2\mathbb{Z}, km + 3\mathbb{Z})$

$= ((k + 2\mathbb{Z}).(m + 2\mathbb{Z}), (k + 3\mathbb{Z}).(m + 3\mathbb{Z}))$

$= ((\mathrm{k} + 2\mathbb{Z}) . (\mathrm{k} + 3\mathbb{Z}), (\mathrm{m} + 2\mathbb{Z}) . (\mathrm{m} + 3\mathbb{Z}))$
$= \psi\big((k + 6\mathbb{Z}) . \psi(m + 6\mathbb{Z})\big)$

په نتيجه کې ψ يو R-Hom دی. د مثال په ډول د $\bar{3}, \bar{4} \epsilon \mathbb{Z}_6$ لپاره امتحان کوو.
د $\mathbb{Z}_2$ ، $\mathbb{Z}_3$ او $\mathbb{Z}_6$ دعناصرومشخص کولولپاره مونږهغوی په لاندې ډول ښيوو:

$\mathbb{Z}_2 = \{ \bar{0}, \bar{1} \} = \{[0]_2 , [1]_2 \}$

$\mathbb{Z}_3 = \{ \bar{0}, \bar{1}, \bar{2} \} = \{[0]_3 , [1]_3 , [2]_3 \}$

$\mathbb{Z}_6 = \left\{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \right\} = \{[0]_6 , [1]_6 , [2]_6 , [3]_6 , [4]_6 , [5]_6 \}$

$[0]_6 = \{0 + 6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z} \} , [1]_6 = \{1 + 6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z} \} ,$

$[2]_6 = \{2 + 6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z} \} , [3]_6 = \{3 + 6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z} \} ,$

$[4]_6 = \{4 + 6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z} \} , [5]_6 = \{5 + 6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z} \}$

$\psi\big((3 + 6\mathbb{Z}) + (4 + 6\mathbb{Z})\big) = \psi(\bar{3} + \bar{4}) = \psi(\bar{1}) = \psi(1 + 6\mathbb{Z})$
$= (1 + 2\mathbb{Z} , 1 + 3\mathbb{Z})$
$\psi(3 + 6\mathbb{Z}) = (3 + 2\mathbb{Z} , 3 + 3\mathbb{Z})$
$\psi(4 + 6\mathbb{Z}) = (4 + 2\mathbb{Z} , 4 + 3\mathbb{Z})$
$\psi(3 + 6\mathbb{Z}) + \psi(4 + 6\mathbb{Z})$
$= (3 + 2\mathbb{Z} , 3 + 3\mathbb{Z}) + (4 + 2\mathbb{Z} , 4 + 3\mathbb{Z})$
$= (7 + 2\mathbb{Z} , 7 + 3\mathbb{Z}) = ([7]_2 , [7]_3)$
$= ([1]_2 , [1]_3 = (1 + 2\mathbb{Z} , 1 + 3\mathbb{Z})$
$= \psi\big((3 + 6\mathbb{Z}) + (4 + 6\mathbb{Z})\big)$
$\psi\big((3 + 6\mathbb{Z}) . (4 + 6\mathbb{Z})\big) = \psi(\bar{3} . \bar{4}) = \psi(\overline{12}) = \psi(\bar{0})$
$= \psi(0 + 6\mathbb{Z})$
$= (0 + 2\mathbb{Z} , 0 + 3\mathbb{Z})$
$\psi(3 + 6\mathbb{Z}) . \psi(4 + 6\mathbb{Z})$
$= (3 + 2\mathbb{Z} , 3 + 3\mathbb{Z}) . (4 + 2\mathbb{Z} , 4 + 3\mathbb{Z})$
$= (12 + 2\mathbb{Z} , 12 + 3\mathbb{Z}) = ([12]_2 , [12]_3)$
$= ([0]_2 , [0]_3 = (0 + 2\mathbb{Z} , 0 + 3\mathbb{Z})$
$= \psi\big((3 + 6\mathbb{Z}) . (4 + 6\mathbb{Z})\big)$

ثبوت شو چه ψ د $\bar{3}, \bar{4} \epsilon \mathbb{Z}_6$ لپاره R-Hom ده.

مثال: $r_1 = 2, r_2 = 4$ لپاره د 4.2 لیما صدق نه کوي. ځکه 4 پر 2 قابل د تقسیم دی. مونږ.بنیو چه ψ یو R-Isom نه ده

$$r = r_1 . r_2 = 2.4 = 8$$
$$\psi : \mathbb{Z}_8 \quad \rightarrow \mathbb{Z}_2 \mathrm{x}\, \mathbb{Z}_4$$
$$k + 8\mathbb{Z} \mapsto (k + 2\mathbb{Z}, k + 4\mathbb{Z})$$ د

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\} = \{[0]_2, [1]_2\}$$

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \{[0]_4, [1]_4, [2]_4, [\bar{3}]\}$$

$$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$$
$$= \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$$
$$[0]_8 = \{0 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}, \quad [1]_8 = \{1 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\},$$

$$[2]_8 = \{2 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\} \; [3]_8 = \{3 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\},$$

$$[4]_8 = \{4 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}, [5]_8 = \{5 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}$$
$$[6]_8 = \{6 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}, \quad [7]_8 = \{7 + 8\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}$$

د ψ تابع اینجکتیف نه ده. ځکه:

$$\psi(2 + 8\mathbb{Z}) = (2 + 2\mathbb{Z}, 2 + 4\mathbb{Z}) = ([2]_2, [2]_4)$$
$$= ([0]_2, [2]_4)$$
$$= (0 + 2\mathbb{Z}, 2 + 4\mathbb{Z})$$
$$\psi(6 + 8\mathbb{Z}) = (6 + 2\mathbb{Z}, 6 + 4\mathbb{Z}) = ([6]_2, [6]_4)$$
$$= ([0]_2, [2]_4) = (0 + 2\mathbb{Z}, 2 + 4\mathbb{Z})$$
$$= \psi(2 + 8\mathbb{Z})$$

مگر $2 + 8\mathbb{Z} \neq 6 + 8\mathbb{Z}$ دی. پس ψ یو injective نه دی

قضیه 4.1 : (Chinese remainder theorem)

که مونږ.اعداد دلاندي خواصو سره ولرو :

(i)

$$r_1, r_2, \ldots, r_n \in \mathbb{N}, \left(r_i \neq 0 \; (i = 1,2, \ldots, n)\right)$$
$$\wedge \; (r_i \nmid r_j \; (i, j = 1,2, \ldots n), i \neq j)$$
($\gcd(r_i, r_j) = 1 \quad (i, j = 1,2, \ldots, n \; \wedge \; i \neq j)$:یعنی)

(ii) $a_1, a_2, \ldots, a_n \in \mathbb{Z}$

بیا:

$$\exists! k \in \mathbb{Z} ; \; \mathrm{k} \equiv \mathrm{a_i} (\mathrm{mod}\, \mathrm{r_i}) \quad (\mathrm{i} = 1,2, \ldots, \mathrm{n})$$

ثبوت:

$a_i + r_i\mathbb{Z} \in \mathbb{Z}_{r_i} \quad (i = 1,2, \dots , n)$

$(a_1 + r_1\mathbb{Z} , a_2 + r_2\mathbb{Z}, \dots \dots , a_n + r_n\mathbb{Z}) \in \mathbb{Z}_{r_1} \mathrm{x}\, \mathbb{Z}_{r_2} \mathrm{x} \dots . \mathrm{x}\, \mathbb{Z}_{r_n}$

په 4.2 لیما کي مووليدل چي دالاندي تابع سورجتيکتيف (surjective) ده:

$$\psi: \mathbb{Z}_{r_1 . r_2 \dots r_n} \longrightarrow \mathbb{Z}_{r_1} \mathrm{x}\, \mathbb{Z}_{r_2} \mathrm{x} \dots . \mathrm{x}\, \mathbb{Z}_{r_n}$$

$$m + r_1 . r_2 \dots r_n\mathbb{Z} \longmapsto (m + r_1\mathbb{Z}, m + r_2\mathbb{Z}, \dots . , m + r_n\mathbb{Z})$$

پس:

$\exists k \in \mathbb{Z}$;

$\psi(k + r_1 . r_2 \dots r_n\mathbb{Z}) = (a_1 + r_1\mathbb{Z} , a_2 + r_2\mathbb{Z}, \dots \dots , a_n + r_n\mathbb{Z}$

له بلي خواد ψ د تعريف له مخي :

$$\psi(k + r_1 . r_2 \dots r_n\mathbb{Z}) = (k + r_1\mathbb{Z}, k + r_2\mathbb{Z}, \dots . , k + r_n\mathbb{Z})$$

په نتيجه کی:

$$k + r_i\mathbb{Z} = a_i + r_i\mathbb{Z} \ \ (i = 1,2, \dots , n)$$

$\Longrightarrow \ k \equiv a_i (\mathrm{mod}\, r_i) \quad (i = 1,2, \dots , n)$ [د 3.12 لیما له مخی]

له بلي خواځرنګه چه ψ اينجکتيف هم دی، پس فقط يواځي يو هغه ډول k موجوده ده

:solve equations of congruent classes

(باقی کلاسو دمعادلاتو حل)

د congruent classes معاودلاتود حل لپاره د Chinese remainder قضيي څخه استفاده کوو.

مونږ دالاندي معادلي لرو :

$\mathrm{X} \equiv a_1 (\mathrm{mod}\, r_1) , \mathrm{X} \equiv a_2 (\mathrm{mod}\, r_2) , \dots , \mathrm{X} \equiv a_n (\mathrm{mod}\, r_n)$

$r_{1,} r_{2,} \dots . , r_n \in \mathbb{N}$; $\gcd(r_{i,} r_j) = 1 \quad (i, j = 1,2, \dots , n \ \wedge \ \ i \neq j)$

$a_{1,} a_{2,} \dots . , a_n \in \mathbb{Z}$

پورتني معادلي کولای شوپه لاندي طريقه حل کړو:

$$r \coloneqq r_1 . r_2 . r_3 . \dots . . r_n \quad , s_i \coloneqq \frac{r}{r_i} \qquad (i = 1,2, \dots , n)$$

اوس $k_i \in \mathbb{Z}$ دلاندي خواصو سره پيده کوو:

$$k_i . s_i \equiv 1 (\mathrm{mod}\, r_i) \qquad (i = 1,2, \dots , n)$$

ځرنګه چه $\gcd(r_{i,} s_i) = 1$ دی، پس د euclidean algorithm له مخی کولای شو k_i په لاندي ډول پيداکړو :

$\exists k_i, m_i \in \mathbb{Z}\,;\;\; k_i\,.\,s_i + m_i.\,r_i = 1 \quad (i = 1,2, \dots, n)$
$k \coloneqq k_1\,.\,s_1\,.\,a_1 + \; k_2\,.\,s_2\,.\,a_2 + \; \dots.+ k_n\,.\,s_n\,.\,a_n$

دپورتنیومعادلاتو حل د $k + r\mathbb{Z}$ سیت دی. یعني:

$$X = \{k + r.\,n | n \in \mathbb{Z}\}$$

مثال: غواړو دلاندي معادلوحل پیدا کړو:

$X \;\equiv 1(\mathrm{mod}\;2)\;\;, \qquad X \;\equiv\; 2(\mathrm{mod}\;3)$

دلته:

$a_1 \;= 1\,, a_2 \;= 2$
$r_1 \;= 2\,, r_2 \;= 3$
$r\!:= \; r_1\,.\,r_2 \;= 2.3 \;= 6$
$s_1 \;= \;\frac{r}{r_1} = \;\frac{6}{2} = 3 \;\;, s_2 \;= \;\frac{r}{r_2} = \;\frac{6}{3} = 2$

اوس $k_1,\; k_2 \;\in \mathbb{Z}$ دلاندي خواصو سره پیدا کوو:

$k_1\,.\,s_1 \;\equiv\; 1(\mathrm{mod}\; r_1\,) \Longrightarrow\; k_1\,.\,3 \;\equiv\; 1(\mathrm{mod}\;2)$
$k_2\,.\,s_2 \;\equiv\; 2(\mathrm{mod}\; r_2\,) \Longrightarrow\; k_2\,.\,2 \;\equiv\; 2(\mathrm{mod}\;3)$

څرنګه چه $\gcd\big(\,r_{i,}\; s_i\,\big) = 1$ دی، پس د euclidean algorithm له مخی کولای شو k_i په لاندي ډول پیداکړو :

$\exists k_i, m_i \in \mathbb{Z}\,;\;\; k_i\,.\,s_i + m_i.\,r_i = 1 \quad (i = 1,2)$
$\gcd(2,3) = \;\gcd(3,2) = 1$

$3 = 1.2 + 1$
$2 = 1.2 + 0$
$1 = 3 - 1.2$
$k_1\,.\,3 + m_1.\,2 = 1$
$k_1 \,= 1$

$k_2\,.\,2 + m_2.\,3 = 1$
$k_1 \,= -1{=}2 \qquad [\;1{+}2 = 0 \Longrightarrow 2 = \;-1$: ځکه $]$

په نتیجه کي:

$k_1 = 1\,, k_2 = 2$
$k = k_1\,.\,s_1\,.\,a_1 + \; k_2\,.\,s_2\,.\,a_2 \;\; = 1.3.1 + 2.2.2 \;\;= 11$
$k + r\mathbb{Z} = 11 + 6\mathbb{Z} = 1.6 + 5 + 6\mathbb{Z} = \;0 + 5 + 6\mathbb{Z}$

معادلاتودحل سیت په لاندي ډول دی:

$$X = \{5 + 6n \mid n\epsilon\mathbb{Z}\}$$

دمثال په ډول د $n = 2$ لپاره يي حل $17 = 6.2 + 5$ دی. ځکه:

$17 = 2.8 + 1 = \Longrightarrow 17 \equiv 1(\mathrm{mod}\ 2)$
$17 = 3.5 + 2 = \Longrightarrow 17 \equiv 2(\mathrm{mod}\ 3)$

مثال: غواړو دلاندي معادلوحل پيدا کړو:

$X \equiv 2(\mathrm{mod}\ 3)\ , \qquad X \equiv 3(\mathrm{mod}\ 5)\ , \qquad X \equiv 2(\mathrm{mod}\ 7)$

دلته:

$a_1 = 2\ , a_2 = 3\ , a_3 = 2$
$r_1 = 3\ , r_2 = 5\ , r_3 = 7$
$r := r_1 . r_2 . r_3 = 3.5.7 = 105$
$s_1 = \frac{r}{r_1} = \frac{105}{3} = 35\ , s_2 = \frac{r}{r_2} = \frac{105}{5} = 21\ ,\ s_3 = \frac{r}{r_3} = \frac{105}{7} = 15$

اوس $k_1, k_2, k_3 \in \mathbb{Z}$ دلاندي خواصو سره پيدا کوو:

$k_1 . s_1 \equiv 1(\mathrm{mod}\ r_1) \Longrightarrow k_1 . 35 \equiv 1(\mathrm{mod}\ 3)$
$k_2 . s_2 \equiv 1(\mathrm{mod}\ r_2) \Longrightarrow k_2 . 21 \equiv 1(\mathrm{mod}\ 5)$
$k_3 . s_3 \equiv 1(\mathrm{mod}\ r_3) \Longrightarrow k_3 . 15 \equiv 1(\mathrm{mod}\ 7)$

څرنګه چه $\gcd(r_{i,}\ s_i) = 1$ دی، پس د euclidean algorithm له مخی کولای شو k_i په لاندي ډول پيداکړو :

$\exists k_i, m_i \in \mathbb{Z}\ ;\ k_i . s_i + m_i . r_i = 1 \quad (i = 1,2,3)$

$k_1 . 35 + m_1 . 3 = 1$

$35 = 11.3 + 2$
$3 = 1.2 + 1$
$2 = 1.2 + 0$
$1 = 3 - 1.2 = 3 - 1.(35 - 11.3) = 12.3 - 1.35$
$k_1 = -1 = 2 \qquad [\ 1+2 = 0 \Longrightarrow 2 = -1\ :$ ځکه $]$

$k_2 . 21 + m_1 . 5 = 1$
$21 = 4.5 + 1$
$4 = 1.4 + 0$

$1 = 21 - 4.5 \ = 1.21 - 4.5 \Longrightarrow \ k_2 = 1$

$k_3\ .15 + m_3.7 = 1$
$15 = 2.7 + 1$
$7 = 1.7 + 0$

$1 = 15 - 2.7 \ = 1.15 - 2.7 \Longrightarrow \ k_3 = 1$

په نتيجه کي:

$k_1 = 2\ ,k_2 = 1\ ,k_3 = 1$
$k = k_1\ .s_1\ .a_1 + \ k_2\ .s_2\ .a_2 + \ k_3\ .s_3\ .a_3$
$= 2.35.2 + 1.21.3 + 1.15.2 = 233$
$k + r\mathbb{Z} = 233 + 105\mathbb{Z} = 2.105 + 23 + 105\mathbb{Z} = \ 23 + 105\mathbb{Z}$

معادلاتودحل سيت په لاندي ډول دی:

$X = \{23 + 105n \mid n\epsilon\mathbb{Z}\ \}$

دمثال په ډول د $n = 1$ لپاره يي حل $128 = 105.1 + 23$ دی. ځکه:

$128 = 42.3 + 2 \ \Longrightarrow 128 \ \equiv \ 2(\mathrm{mod}\ 3)$
$128 = 25.5 + 3 \ \Longrightarrow 128 \ \equiv \ 3(\mathrm{mod}\ 5)$
$128 = 18.7 + 2 \ \Longrightarrow 128 \ \equiv \ 2(\mathrm{mod}\ 7)$

د $n = -1$ لپاره يي حل $-82 = 23 - 105 = 23 + 105.(-1)$ دی ځکه:

$-82 = (-28).3 + 2 \ \Longrightarrow -82 \ \equiv \ 2(\mathrm{mod}\ 3)$
$-82 = (-17).5 + 3 \ \Longrightarrow -82 \ \equiv \ 3(\mathrm{mod}\ 5)$
$-82 = (-12).7 + 2 \ \Longrightarrow -82 \ \equiv \ 2(\mathrm{mod}\ 7)$

مثال: ديوښوونځي سرمعلم غواړی د زدکونکی په قطارودروی.
که قطار 3 کسيزه وي، بيا 2 زدکونکي باقی پاتي کيږي
که قطار4 کسيزه وي ، بيا 1 شاګرد باقی پاتي کيږي
که قطار7 نفره وي، بيا هيڅ شاګرد باقی نه پاتی کيږي
معلوم کړی چه د شاګردانو شمير په هغه مکتب کي اقلاًڅودی

حل: که ښوونځي دشاګردانوشمير k وی، بيايی معادلاتي کلاسونه لاندي شکل لری:

$k \ \equiv \ 2(\mathrm{mod}\ 3)\ \ , \qquad k \ \equiv \ 1(\mathrm{mod}\ 4)\ , \qquad k \ \equiv \ 0\ (\mathrm{mod}\ 7)$

دلته:

$a_1 = 2, a_2 = 1, a_3 = 0$
$r_1 = 3, r_2 = 4, r_3 = 7$
$r = r_1 . r_2 . r_3 = 3.4.7 = 84$

$$s_1 = \frac{r}{r_1} = \frac{r_1 . r_2 . r_3}{r_1} = r_2 . r_3 = 4.7 = 28$$

$$s_2 = \frac{r}{r_2} = \frac{r_1 . r_2 . r_3}{r_2} = r_1 . r_3 = 3.7 = 21$$

$$s_3 = \frac{r}{r_3} = \frac{r_1 . r_2 . r_3}{r_3} = r_1 . r_2 = 3.4 = 12$$

اوس $k_1, k_2, k_3 \in \mathbb{Z}$ دلاندي خواصو سره پيدا کوو:

$k_1 . s_1 \equiv 1 (\mathrm{mod}\ r_1) \Rightarrow k_1 . 28 \equiv 1 (\mathrm{mod}\ 3)$

$k_2 . s_2 \equiv 1 (\mathrm{mod}\ r_2) \Rightarrow k_2 . 21 \equiv 1 (\mathrm{mod}\ 4)$

$k_3 . s_3 \equiv 1 (\mathrm{mod}\ r_3) \Rightarrow k_3 . 12 \equiv 1 (\mathrm{mod}\ 7)$

ځرنګه چه $\gcd(r_i, s_i) = 1$ دی، پس د euclidean algorithm له مخې k_i کولای شو په لاندي ډول پيداکړو :

$\exists k_i, m_i \in \mathbb{Z}; \ k_i . s_i + m_i . r_i = 1 \quad (i = 1,2,3)$

$k_1 . 28 + m_1 . 3 = 1$
$28 = 9.3 + 1$
$3 = 1.3 + 0$
$1 = 28 - 9.3 \Rightarrow k_1 = 1$

$k_2 . 21 + m_2 . 4 = 1$

$21 = 5.4 + 1$
$4 = 1.4 + 0$
$1 = 21 - 5.4 \Rightarrow k_2 = 1$

$k_3 . 12 + m_3 . 7 = 1$

$12 = 1.7 + 5$
$7 = 1.5 + 2$
$5 = 2.2 + 1$
$2 = 1.2 + 0$

$1 = 5 - 2.2$
$\quad = 5 - 2.(\,7 - 1.5) = 5 - 2.(\,7 - 1.(12 - 1.7))$
$\quad = 12 - 1.7 - 2.7 + 2.12 - 2.7 = 3.12 - 5.7$

$\Longrightarrow k_3 = 3$

$k = k_1 . s_1 . a_1 + k_2 . s_2 . a_2 + k_3 . s_3 . a_3$
$\qquad = 1.28.2 + 1.21.1 + 3.12.0 = 77$

د معادلات یو حل 77 دی. یعنی هغه مکتب اقلاً 77 شاګردان لري . ځکه دالاندي روابط صدق کوي:

$77 \equiv 2(\mathrm{mod}\ 3)\ , \qquad 77 \equiv 1(\mathrm{mod}\ 4)\ , \qquad 77 \equiv 0\ (\mathrm{mod}\ 7)$

دهغومعادلات عمومی حل په لاندي دی:

$k + r\mathbb{Z} = 77 + 84\mathbb{Z}$

د حل سیټ يي که په X سره وښیوو

$X = \{77 + 84n \mid n\epsilon\mathbb{Z}\ \}$

د امتحان لپاره که $n = 1$ وي، بیا:

$k = 77 + 84.1 = 161$

ځکه:

$161 = 53.3 + 2 \Longrightarrow 161 \equiv 2(\mathrm{mod}\ 3)$
$161 = 40.4 + 1 \Longrightarrow 161 \equiv 1(\mathrm{mod}\ 4)$
$161 = 23.7 + 0 \Longrightarrow 161 \equiv 0\ (\mathrm{mod}\ 7)$

تمرین: دلاندي معادلوحل پیدا کړي:

$X \equiv 1(\mathrm{mod}\ 2)\ , X \equiv 2(\mathrm{mod}\ 3)\ , X \equiv 1(\mathrm{mod}\ 4)$

پنځم فصل

دورانی ګروپونه (cyclic groups)

(G , .) یوګروپ چې e دهغه عینیت عنصردی او a ∈G . د G یو فرعی ګروپ چې مولد (generator) یې a وې په <a> سره ښیو. یعنې

$<a> = \{a^k | \ k \in \mathbb{Z}\}$

قضیه 5.1: (G , .) یو ګروپ چې e∈ G یې عینیت عنصر (identity) دی ، a∈ G

(a) که ord(a) = n معین وې. بیا په دی صورت :

(i) $\mathrm{Ord(a)} = |< a >| \ \wedge < a > = \{ e , \mathrm{a}^1, \mathrm{a}^2, \ldots , \mathrm{a}^{\mathrm{n}-1}\}$

(ii) $a^s = e \Leftrightarrow ord(a) \big| \ s$

(b) که ord(a) = ∞ وی. بیا :

$\forall \, i,j \in \mathbb{N} , i \neq j \Longrightarrow a^i \neq a^j$

(a) **ثبوت** : ځرنګه چې ord(a) = n دی پس n ترټولوکوچنی طبعی عدد دی چې $a^n = e$ شي .

د H سیت داډول تعریف کوو : $\mathrm{H}: = \{\mathrm{k} \in \mathbb{Z} \mid \mathrm{a}^{\mathrm{k}} = \mathrm{e}\}$

H د$(\mathbb{Z} , +)$ یو فرعی ګروپ دی . ځکه:

$\mathrm{n} \in \mathrm{H} \Longrightarrow \mathrm{H} \neq \emptyset$

$\mathrm{k, m} \in \mathrm{H} \Longrightarrow \mathrm{a}^{\mathrm{k}} = \mathrm{a}^{\mathrm{m}} = \mathrm{e} \Longrightarrow \mathrm{a}^{\mathrm{k}}.\mathrm{a}^{-\mathrm{m}} = \mathrm{a}^{\mathrm{k}-\mathrm{m}} = \mathrm{e}$

$\Longrightarrow \mathrm{k} + (-\mathrm{m}) \in \mathrm{H}$

پس د 3.2 قضیې له مخې H یو فرعي ګروپ د $(\mathbb{Z} , +)$ دی. د 3.6 قضیې له مخې باید H = n$\mathbb{Z}$ وي او n ترټولوکوچنی طبعی عدد دی چې $a^n = e$.

د division algorithm په اساس:

$\mathrm{m} \in \mathbb{Z}$

$\Longrightarrow \ \exists \mathrm{q, r} \in \mathbb{Z} \, ; \ \mathrm{m} = \mathrm{q.n} + \mathrm{r} \quad 0 \leq \mathrm{r} < n$

$\Longrightarrow \ a^m = (a^n)^{q+r} = (a^n)^q \ .a^r = e \ a^r = a^r$

$\Longrightarrow \ a^m = a^r \in \{ \mathrm{e}, a^1, a^2, . \ . \ . \ , a^{n-1}\}$ [ځکه r < n دی]

لیدل کیږي چې دهر $m\in \mathbb{Z}$ لپاره a^m په $\{ e, a^1, a^2, ... , a^{n-1}\}$ کې واقع دی. پس:

$$< a >= \{a^k \mid k \in \mathbb{Z}\} = \{ e, a^1, a^2, ... , a^{n-1}\}$$

خرنګه چې $|< a >| = n$ دی پس $ord(a) = |< a >|$. په نتیجه کې (i) ثبوت شو.

(ii) ثبوت :

"$\Leftarrow$"

$$ord(a) = n|s \Rightarrow \exists q \in \mathbb{N} \ ; s = q . n$$
$$\Rightarrow a^s = a^{q.n} = (a^n)^q = (e)^q = e$$

"$\Rightarrow$"

$$a^s = e \Rightarrow s \in \{k \in \mathbb{Z} \mid a^k = e\} = n . \mathbb{Z}$$
$$\Rightarrow \exists z \in \mathbb{Z}; s = n. z \Rightarrow n|s$$

(b) ثبوت: که هغه ډول نه وي پس باید j او i موجود وي چې $i \neq j$ مګر $a^i = a^j$ شي . البته دلته i او j طبعی اعداد دي . مونږ فرض کوچې $i < j$ صدق کوي :

$$a^i = a^j \Rightarrow a^{i-j} = e$$

له دې څخه نتیجه اخلوچې یو عدد k پیدا شو چې $a^k = e$ شي . پس باید *ord(a)* معین وي . مګردا دفرضي تضاد سره چې *ord(a)=* ∞ دی ، واقع کیږي. پس باید:

$$\forall \ i,j \in \mathbb{N} , i \neq j \Rightarrow a^i \neq a^j$$

لیما 5.1 : (G, .) او $(G_1,*)$ دوه ګروپه چې $e \in G$ او $e_1 \in G_1$ یې عینیت عناصردي. $a \in G$ معینه مرتبه (order) لري او $\varphi: G \longrightarrow \mathbf{G_1}$ یو G-Hom دی. بیا:

(a) $ord(\varphi(a)) | ord (a)$

(b) $\varphi \text{ injective} \Rightarrow ord(\varphi(a)) = ord(a)$

(a) ثبوت : خرنګه چې φ یو G-Hom دی پس لیکلی شو :

$$(\varphi(a))^{ord(a)} = (\varphi(a)) * \varphi(a) * ....$$
$$* \varphi(a)) \quad [\ (\text{دفعه}) \text{ واري } ord(a)\ ]$$
$$= \varphi (a . a . ... .a) \quad [\ (\text{دفعه}) \text{ واري } ord(a)\ ]$$
$$= \varphi(a^{ord(a)})$$
$$= \varphi (e) = e_1 \qquad [\ \text{قضیې له مخې } 2.1\ ]$$

$\Longrightarrow \text{ord}(\varphi(a)) | \text{ord}(a)$ [قضيې له مخې 5.1]

ثبوت (b):

$(\varphi(a))^{ord(\varphi(a))}$

$= (\varphi(a)) * \varphi(a) * \ldots.$

$* \varphi(a)$) [(دفعه) واري $ord(\varphi(a))$]

$= \varphi$ (a . a . … .a) [a واري $ord(\varphi(a))$]

$= \varphi\ (a^{ord(\varphi(a))})$

$\Longrightarrow\ e_1 = (\varphi(a))^{ord(\varphi(a))} = \varphi\ (a^{ord(\varphi(a))})$

له بلې خوا:

$\varphi(e) = e_1 \quad \Longrightarrow\ \varphi\ (a^{ord(\varphi(a))}) = e_1 = \varphi(e)$

$\Longrightarrow\ a^{ord(\varphi(a))} = e$ [injective φ ځکه]

پس د 5.1 قضيې له مخې باید $\text{ord}(a) | \text{ord}(\varphi(a))$ او د (a) له مخې

$ord(\varphi(a)) | ord(a)$ وې. په نتیجه کې $\text{ord}(\varphi(a)) = \text{ord}(a)$

لیما 5.2 : (. ,G) یوکروپ او $e \in G$ دهغه عینیت عنصر دی .که د $a \in G$

لپاره $a^0 := e$ او $(a^{-i}) := (a^i)^{-1}$ تعریف کړو. بیا:

$< a > = \{ a^i \mid i \in \mathbb{Z} \}$ یو فرعی ګروپ د G دی .

ثبوت :

$i = 0\ ,\ a^0 = e \in < a > \Longrightarrow < a > \neq 0$

$x, y \in < a > \Longrightarrow \exists\, m, n \in \mathbb{Z}\ ; x = a^m \wedge y = a^n$

$\Longrightarrow x \,.\, y^{-1} = a^m \,.\, (a^n)^{-1}$

$= a^m \,.\, a^{-n} = a^{m-n}$

$\Longrightarrow x \,.\, y^{-1} \in < a >$

په نتیجه کې <a> د 3.2 قضیې له مخې یو فرعی ګروپ د G دی چې په عین وخت کې دورانی ګروپ هم دی .

مثال: پدی مثال کی د پورتنی لیما ِڅخه استفاده کوو

(a) غواړو د <f> فرعی ګروپ په Q_6 پیدا کړو

$f^0 = e\ ,\ f^1 = f\ ,\ f^2 = e \Longrightarrow \ <f> = \{ e, f \}$

(b) غواړو د <d> فرعی ګروپ په Q_8 کی پیدا کړو

$d^1 = d\ ,\ d^2 = a\ ,\ d^3 = a.d = f\ ,\ d^4 = f.d = e$

$\Longrightarrow\ <d> = \{ e, a, d, f \}$

(c) غواړو د $<\bar{5}>$ فرعی ګروپ په $(\mathbb{Z}_7^*, .)$ کی پیدا کړو

$(\bar{5})^1 = \bar{5}$, $(\bar{5})^2 = (\overline{25}) = \bar{4}$, $(\bar{5})^4 = \bar{4}.\bar{5} = \overline{20} = \bar{6}$,
$(\bar{5})^5 = \bar{6}.\bar{5} = \overline{30} = \bar{2}$, $(\bar{5})^6 = \bar{2}.\bar{5} = \overline{10} = \bar{3}$,
$(\bar{5})^7 = \bar{3}.\bar{5} = \overline{15} = \bar{1}$
$\Longrightarrow \; <\bar{5}> = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \mathbb{Z}_7^*$

تمرین: د حل لپاره د 5.2 لیما څخه استفاده وکړئ .
(a) د <b> فرعی ګروپ په D_4 ، Q_6 او Q_8 کې پیدا کړئ
(b) د <k> او <-I> فرعي ګروپونه په Q کې پیدا کړئ
(c) د $<\bar{3}>$ فرعی ګروپ په $(\mathbb{Z}_5^*,.)$, $(\mathbb{Z}_{11}^*,.)$ او $(\mathbb{Z}_{13}^*,.)$ کې پیدا کړئ

قضیه 5. 2: هر فرعی ګروپ د یو دورانی ګروپ (cyclic group) هم دورانی دی .

ثبوت : که (. , G) یو دورانی ګروپ چې $< x > = G$ او $e \in G$ یی عینیت عنصر وي. مونږ فرضووچې H یو فرعی ګروپ د G دی.

لمړی حالت : H={e} په دي صورت H=<e> دورانی دی .

دویم حالت : $\mathbf{H \neq \{e\}}$

$H \neq \{e\} \Longrightarrow \exists y \in H , y \neq e$
$\Longrightarrow \exists m > 0 \,; y = x^m$ [$y \in G$ ځکه]

اوس ترټولوکوچنی m انتخابوو،چې $x^m \in H$ وي.څرنګه چې H یوفرعي ګروپ دی پس:

$x^m \in H \;\Longrightarrow\; x^m , (x^m)^2 , (x^m)^3 , \ldots \in H$
$\Longrightarrow < x^m > \subseteq H$

اوس غواړوثبوت چې $H \subseteq < x^m >$ دی .

$h \in H \Longrightarrow \exists\, i \in \mathbb{Z} \,; h = x^i$
$\Longrightarrow \exists q, r \in \mathbb{Z} \,; i = mq + r \,,\; 0 \leq r < m$
$\Longrightarrow x^i = x^{mq+r} = x^{mq}.x^r$
$\Longrightarrow x^r = x^i.x^{-mq} \in H$ [$x^m , x^i \in H$ ځکه]

څرنګه چې مو *m* ترټولوکوچنی عدد په $x^m \in H$ کی انتخاب کړی وه.
مګرګوروچې r < m او $x^r \in H$ دی .پس باید *r = 0* وې .

$r = 0 \Longrightarrow i = mq \Longrightarrow x^i = (x^m)^q \in < x^m >$
$\Longrightarrow H \subseteq < x^m >$

ثبوت شو چې $H = < x^m >$ یو دورانی ګروپ دی .

مثال 5.1 : $(\mathbb{Z}_7^*, .)$ یودورانی (cyclic) ګروپ دی اومولد **(generator)** یي $\bar{3}$ دی. یعني $\mathbb{Z}_7^* = <\bar{\mathbf{3}}>$. ځکه:

$ord(\mathbb{Z}_7^*) = |\mathbb{Z}_7^*| = 6 \quad , \ \mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$(\bar{3})^1 = \bar{3}$
$(\bar{3})^2 = \bar{9} = \bar{7} + \bar{2} = \bar{2}$
$(\bar{3})^3 = \bar{2}.\bar{3} = \bar{6}$
$(\bar{3})^4 = \bar{6}.\bar{3} = \overline{18} = \overline{2.7} + \bar{4} = \bar{4}$
$(\bar{3})^5 = \bar{4}.\bar{3} = \overline{12} = \bar{7} + \bar{5} = \bar{5}$
$(\bar{3})^6 = \bar{5}.\bar{3} = \overline{15} = \overline{14} + \bar{1} = \bar{1}$

ثبوت شوچې د $(\bar{3})^i$ (i= 1,2,3,4,5,6) څخه ټول عناصرد $\mathbb{Z}_7^*$ لاس ته راځي.
پس $\mathbb{Z}_7^* =< \bar{3} >$ دی .
$H = \{\bar{1}, \bar{2}, \bar{4}\}$ یو دورانی فرعی ګروپ د $\mathbb{Z}_7^*$ دی .

$(\bar{4})^1 = \bar{4}$
$(\bar{4})^2 = \bar{4}.\bar{4} = \overline{16} = \overline{14} + \bar{2} = \bar{2}$
$(\bar{4})^3 = \bar{2}.\bar{4} = \bar{8} = \bar{7} + \bar{1} = \bar{1}$

په نتیجه کي $H =< \bar{4} >$

تمرین 5.1 : د $(\mathbb{Z}_5^*, .)$ ، $(\mathbb{Z}_5, +)$ ، $(\mathbb{Z}_{11}^*, .)$ ټول فرعی ګروپونه پیدا کړی او ثبوت یی کړی چې دورانی دي.

تمرین 5.2 : $(G_1, *)$ $\longrightarrow$ $\varphi :$ (G,.) یو G - isom او $a \in G$ معینه مرتبه (*order*) لري. بیا

G cyclic (دورانی *)* $\Leftrightarrow$ G_1 cyclic (دورانی *)*

لیما 5.3 : (G , .) = <a> یو دورانی (cyclic) معین ګروپ او $e \in G$ یي عینیت عنصر (identity) دی . که ord(G)=n او n پر یو $d \in \mathbb{N}$ قابل د تقسیم وی . په دې صورت فقط یوازی یو فرعی ګروپ وجود لري چې مرتبه (order) یي مساوی d وې اوهغه فرعی ګروپ $< a^{\frac{n}{d}} >$ دی .

ثبوت : د 5.2 قضیي له مخې $< a^{\frac{n}{d}} >$ یو فرعی ګروپ د G= <a> دی .

$\mathrm{Ord(a)} = |< a >| = \mathrm{n}$
$\Longrightarrow \ \mathrm{a^n = e} \quad [$ ترټولوکوچنی طبعی عدد $n]$
$(a^{\frac{n}{d}})^l \ \ (l = 1,2, \dots, d)$
$\Longrightarrow \ \frac{n}{d}\, l < n \qquad [$ د $l \neq d$ لپاره $]$

$\Longrightarrow \quad a^{\frac{n}{d}.l} \neq e$ [$a^n = e$ ځکه n ترټولوکوچنی عدد دی چې]

$a^{\frac{n}{d}.l} = a^n = e$ [د $l = d$ لپاره]

له دې ځخه نتیجه اخلوچې d ترټولوکوچنی عدد دی چې $(a^{\frac{n}{d}})^d = e$

$\Longrightarrow d = ord(a^{\frac{n}{d}}) = \left|< a^{\frac{n}{d}} >\right|$

اوس غواړو ثبوت کړوچې $< a^{\frac{n}{d}} >$ یوازنی فرعی گروپ د G دی چې مرتبه (order) یې d وې .که H هم همدارنگه یوفرعې گروپ وې چې $ordH = |H| = d$ کیږي. د 5.2 قضی له مخې یو $t \in \mathbb{N}$ موجود دی چې $H = < a^t >$ کیږي

$\Longrightarrow (a^t)^d = e$ [$fermat$ قضیه]

$\Longrightarrow n|\, t.d$ [قضیه 5.1]

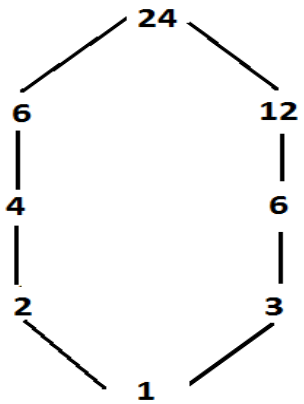
$\Longrightarrow \quad \frac{n}{d}|t \quad \Longrightarrow \quad \frac{n}{d} \leq t$

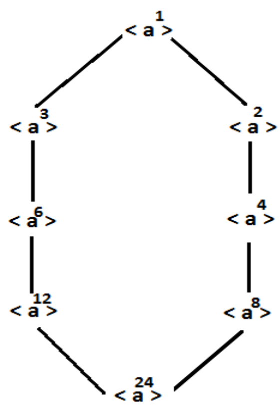
$\Longrightarrow \quad a^t \in < a^{\frac{n}{d}} > \quad \Longrightarrow \quad H \subseteq < a^{\frac{n}{d}} >$

ځرنګه $\left|< a^{\frac{n}{d}} >\right| = d = |H|$ دی. پس $H = (a^{\frac{n}{d}})$

مثال 5.2: که $G=<a>$ یو دورانی گروپ چې $|G| = 24$ وې . بیا ټول هغه اعداد چې 24 پرې قابل د تقسیم وې اوټول فرعی گروپونه د گراف په شکل وښیو

$$G = \{a^1, a^2, \ldots, a^{23}, a^{24} = e\}$$





نوټ : که G یومعین گروپ مګر دورانی نه وي .په دی صورت د ټولو فرعی گروپو تعین یوڅه پیچلی دی . د مثال په ډول $|s_4| = 24$ دی مګرد فرعی گروپو شمیریي 30 دی .

لیما 5.4 : $(G\,,\,.)$ یو دورانی ګروپ چې e عینیت عنصردی . بیا:
(a) که G یو معین (finite) ګروپ وې چې مرتبه (order) یی n ده. بیا
د G او $(\mathbb{Z}_n,+)$ ترمینځ یو G-Isom موجود دی. یعنې $G \cong \mathbb{Z}_n$
(b) که مرتبه (order) د G غیر معین (infinite) وې. په دې صورت د
G او $(\mathbb{Z},+)$ ترمینځ G-Isom موجود دی . یعنې $G \cong \mathbb{Z}$
ثبوت : څرنګه چې G یو دورانی (cyclic) ګروپ دی ، پس یو $a \in G$ موجود
دی چې G=<a> شې .

$$\varphi\colon (\mathbb{Z},+) \longrightarrow (G,.)$$
$$k \longmapsto a^k$$

: $\boldsymbol{\varphi}$ ***surjective***

څرنګه چې G یو دورانی ګروپ دی پس یوه a∈ G موجوده ده چې <a> = G
شې

$$x \in G \implies \exists k \in \mathbb{Z} \;\; ; \quad x = a^k = \varphi(k)$$
$$\implies \varphi \; surjective$$

: **φ G − Hom**

$$k, r \in \mathbb{Z} \;, \varphi(k+r) = a^{k+r} = a^k . a^r = \varphi(k).\varphi(r)$$

Ker φ د 2.4 قضیې له مخې یو فرعی ګروپ د $(\mathbb{Z},+)$ دی .د 3.6 قضیې په
اساس kerφ کولاې شی د $\mathbb{Z}$ د فرعي ګروپ په حیث فقط یوازې
$ker\varphi = \{0\}$ او یا $ker\varphi = n\mathbb{Z}$ ($n \in \mathbb{N}$) شکل ولرې
(a) ثبوت :

$$\mathrm{ord(G) = n \;\wedge\; <a> = G}$$
$$\implies \varphi(n) = \mathrm{a^n = e = a^{2n}} = \varphi(2n) \quad [\text{د } 5.1 \text{ قضیی په اساس}]$$
$$\implies \mathrm{n,2n} \in \mathrm{ker}\varphi$$
$$\implies \ker \varphi \neq \{0\} \quad \implies \ker \varphi = n\mathbb{Z}$$
$$\implies \ker \varphi = n\mathbb{Z}$$

د 3.19 قضیې (همو مورفیزم) له مخې یو G-Isom د $\varphi(\mathbb{Z})$ او $\mathbb{Z}/_{ker\varphi}$

تر مینځ موجود دی . یعنې

$$\mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}/_{ker\varphi} \cong \varphi(\mathbb{Z})$$

څرنګه چې φ یو surjective دی پس باید $\varphi(\mathbb{Z}) = G$ شي . په نتیجه کې

$$\mathbb{Z}/_{\mathrm{n}\mathbb{Z}} = \mathbb{Z}_{\,n} \cong G$$

ثبوت (b)

$\operatorname{ord}(G)=\infty \Longrightarrow \operatorname{Ker}\varphi=\{0\}$ [نظر (a)]

$\Longrightarrow \varphi$ injective [د 2.3 قضیې په اساس]

په نتیجه کی φ یو G-Isom دی. یعنې $G\cong\mathbb{Z}$

قضیه 5.3 : $a_1,a_2,\ \dots,a_n\in\mathbb{Z}^*$ او که $d=\gcd(a_1,a_2,\ \dots,a_n)$ وې بیا :

(a) $<a_1,a_2,\ \dots,a_n>=d\mathbb{Z}$

$$\wedge\ \ \exists\ \ r_1,r_2,\ \dots,r_n\in\mathbb{Z}\,;d=r_1a_1+r_2a_2+\cdots+r_na_n$$

(b) $k|\ a_i\ \ (i=1,2,\dots,n)\Longrightarrow\ k\ |d$

ثبوت (a) : د 3.2 لیما په اساس هر a_i مولد (generator) د $a_i\mathbb{Z}$ دی . پس لهذا کولای شوولیکو :

$$<a_1,a_2,\qquad \dots,a_n>=\ a_1\mathbb{Z}+a_2\mathbb{Z}+\cdots+a_n\mathbb{Z}$$
$$=\{\ \textstyle\sum_{i=1}^{n}s_ia_i\,\big|\ \ s_i\in\mathbb{Z}\ \}$$

خرنګه چې $<a_1,a_2,\ \dots,a_n>$ یو فرعی ګروپ د $(\mathbb{Z},+)$ دی پس یو $k\in\mathbb{Z}$ موجود دی چې :

$$<a_1,a_2,\ \dots,a_n>=k\mathbb{Z}=<k>$$
$$a_i\in<a_1,a_2,\dots,a_n>=k\mathbb{Z}$$
$$\Longrightarrow\ \exists s_i\in\mathbb{Z}\ ;\ a_i=s_ik\quad(i=1,2,\dots,n)$$
$$\Longrightarrow\ k=\ \ cd(a_1,a_2,\dots,a_n)$$

یعنېk یو مشترک قاسم د $a_1,a_2,\dots,a_n$) دی.خرنګه چې $k\in k\mathbb{Z}$ دی . پس :

$$k\in k\mathbb{Z}=a_1\mathbb{Z}+a_2\mathbb{Z}+\cdots+a_n\mathbb{Z}$$
$$\Longrightarrow\ \exists r_1,r_2,\ \dots,r_n\in\mathbb{Z}\ ;k=r_1a_1+r_2a_2+\cdots+r_na_n$$

(b) ثبوت : که m هم یو مشترک قاسم د $a_1,a_2,\ \dots,a_n$ وې . یعنې $m\ =cd(a_1,a_2,\ \dots,a_n)$ پس :

$$m\ |\ a_i\ (i=1,2,\dots,n)\Longrightarrow\ \ m|r_ia_i\quad (i=1,2,\dots,n)$$
$$\Longrightarrow\ m|r_1a_1+r_2a_2+\cdots+r_na_n=k$$
$$\Longrightarrow\ k=\gcd(a_1,a_2,\dots,a_n)$$

خرنګه چه $a_1,a_2,\ \dots,a_n$ فقط یوائې یو لوی مشترک قاسم (gcd) ولری، پس باید:

$$d=\gcd(a_1,a_2,\dots,a_n)=k$$

مثال: خرنګه gcd(9,12) = 3 دی. پس د 5.3 قضیې په اساس لیکی شو

$< 9,12 > = 9\mathbb{Z} + 12\mathbb{Z} = 3\mathbb{Z}$

اوس غواړو پورتنی رابطه ثبوت کړو

$h \in 9\mathbb{Z} + 12\mathbb{Z} \Rightarrow \exists a,b \in \mathbb{Z}\ ;\ h = 9a + 12b = 3(3a+4b)$

$\Rightarrow h \in 3\mathbb{Z} \Rightarrow 9\mathbb{Z} + 12\mathbb{Z} \subseteq 3\mathbb{Z}$

$h \in 3\mathbb{Z} \Rightarrow \exists c \in \mathbb{Z}\ ;\ h = 3c$

$\gcd(9,12) = 3$

$\Rightarrow \exists s,r \in \mathbb{Z}\ ;\ 3 = r.9 + s.12$ [division algorithm]

$\Rightarrow h = 3.c = (r.9 + s.12).c = r.c.9 + s.c.12$

$\Rightarrow h \in 9\mathbb{Z} + 12\mathbb{Z} \Rightarrow 3\mathbb{Z} \subseteq 9\mathbb{Z} + 12\mathbb{Z}$

تمرین 5.3 : یو فرعی ګروپ $d\mathbb{Z}$ په $(\mathbb{Z}\ ,+)$ ګروپ کې پیدا کړی چې

(a) $< 40, 24 ,16 > = d\mathbb{Z}$ وې.

(b) $< 45,12 > = d\mathbb{Z}$ وې.

تعریف 5.1 : $0 \neq a_i \in \mathbb{Z}$ $(i=1,2,\ldots,n)$ اعداد د relatively prime (نسبي لمړنی اعداد) په نوم یادیږي ، که چیري $gcd(a_1, a_2, \ldots, a_n) = 1$ وېي. د 3.7 قضیی له مخې بیا $r_i \in \mathbb{Z}$ $(i=1,2,\ldots,n)$ اعداد د لاندې خواصو سره موجود دي :

$$r_1a_1 + r_2a_2 + \cdots + r_na_n = 1$$

مثال : 5 او 9 له یوبل سره relatively prime (rel -prim) دي. ځکه :

9 = 1* 5 + 4	1 = 5 - 1 * 4
5 =1* 4 + 1	= 5 - 1 * (9 – 1 * 5)
4 = 4 * 1+0	= 2 * 5 - 1 * 9

لیدل کیږي چې gcd(9,5)=1 دی. پس 5 او 9 له یوبل سره relat-prime دي ، r = 2 او s = -1 دي.

لیما 5.6: (G , .) یو ګروپ ، $e \in G$ عینیت عنصر او $a \in G$ معینه مرتبه لري . یعنې ord(a) = n . بیا:

$$\forall\, k \in \mathbb{Z}\ ; \operatorname{ord}(a^k) = \frac{n}{\gcd(n,k)}$$

ثبوت : که $t := ord(a^k)$ او $d := \gcd(n,k)$ وي. په دې صورت:

$a^{kt} = (a^k)^t = e \Rightarrow n \mid tk$ [د 5.1 قضیی]

$\Rightarrow \frac{n}{d} \mid t.\frac{k}{d}$

$\frac{k}{\mathrm{d}}$ او $\frac{n}{\mathrm{d}}$ له یوبل سره relative prime (نسبی لمړني اعداد) دي. ځکه که داسی نه وي. بیا باید یو m∈ ℕ موجود وي چې:

$$\gcd\left(\frac{k}{\mathrm{d}}, \frac{n}{\mathrm{d}}\right) = m \neq 1 \implies m \mid \frac{k}{\mathrm{d}} \wedge m \mid \frac{n}{\mathrm{d}}$$
$$\implies m.d \mid k \wedge m.d \mid n$$

څرنګه چې m.d > d دی. پس d = gcd(k,n) امکان نه لري. مګردا د d د انتخاب خلاف دی. پس باید $\frac{k}{\mathrm{d}}$ او $\frac{n}{\mathrm{d}}$ له یو بل سره relative prime وي

څرنګه چې $\gcd\left(\frac{k}{\mathrm{d}}, \frac{n}{\mathrm{d}}\right) = 1$ او $\frac{n}{\mathrm{d}} \mid t.\frac{k}{\mathrm{d}}$ دی. پس د 3.3 لیما له مخی باید $\frac{n}{\mathrm{d}} \mid t$ صدق وکړي. له دي څخه نتیجه اخلوچې $\frac{n}{\mathrm{d}} \le t$ دی

له بلی خوا :

$$(a^k)^{\frac{n}{\mathrm{d}}} = (a^n)^{\frac{k}{\mathrm{d}}} = (e)^{\frac{k}{\mathrm{d}}} = e$$

څرنګه چې $t = ord(a^k)$ ترټولوکوچنی عدد په ℕ کې دی چې $(a^k)^t = e$ کیږي. پس $t \le \frac{n}{\mathrm{d}}$ دی .

په نتیجه کې:

$$ord(a^k) = t = \frac{n}{\mathrm{d}} = \frac{n}{\gcd(n,k)}$$

مثال 5.4: مونږ د $G = \{a^1, a^2, \dots, a^{24} = e\}$ ګروپ په نظرکې نیسو. $a^3 \in G$

$$< a^3 > = \{ a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24} = e\}$$

د $< a^3 >$ فرعی ګروپ مرتبه 8 ده . یعني $ord(< a^3 >) = 8$ اوهمدارنګه $ord(a^3) = 8$. ځکه :

$a^3, a^3.a^3 = a^6 = (a^3)^2$, $a^6.a^3 = a^9 = (a^3)^3$
$a^9.a^3 = a^{12} = (a^3)^4$, $a^{12}.a^3 = a^{15} = (a^3)^5$
$a^{15}.a^3 = a^{18} = (a^3)^6$, $a^{18}.a^3 = a^{21} = (a^3)^7$
$a^2.a^3 = a^{24} = e = (a^3)^8$

که مونږ k = 6 ولرو :

$(a^3)^6 = a^{18}$
$a^{2.18} = a^{18}.a^{18} = a^{36} = a^{24}.a^{12} = e.a^{12} = a^{12}$
$a^{3.18} = a^{12}.a^{18} = a^{30} = a^{24}.a^6 = a^6$
$a^{4.18} = a^{3.18}.a^{18} = a^6.a^{18} = a^{24} = e$

لیدل کیږي چې $ord(a^3)^6 = 4$ کیږي . که پورتنی لیما تطبیق کړو. بیا هم عین نتیجه لاسته راځي :

$$ord((a^3)^6) = \frac{ord(a^3)}{\gcd(ord(a^3),6)} = \frac{8}{\gcd(8,6)} = \frac{8}{2} = 4$$

لیما 5.7: که $(G\ ,.) = <a>$ یو دورانی (cyclic) ګروپ وي چې n متناهی مرتبه (finite order) ولري . په دې صورت بیا دهر $k \in \mathbb{Z}$ لپاره دالاندي افاده صدق کوې :

$$G =< a^k > \iff \gcd(n,k) = 1$$

ثبوت " $\Longrightarrow$ "

$$< a > = G = < a^k > \Longrightarrow ord\ (a^k) = n$$

په 5.6 لیما کې مو ولیدل چې :

$$ord\ (a^k) = \frac{n}{\gcd(n,k)}$$

$$\Longrightarrow n = \frac{n}{\gcd(n,k)} \Longrightarrow \gcd(n,k) = \frac{n}{n} = 1$$

" $\Longleftarrow$ "

په 5.6 لیما کې ولیدل شول چې $ord\ (a^k) = \frac{n}{\gcd(n,k)}$ اودفرضی له مخې $\gcd(n\ ,k) = 1$ دی. پس $ord(a^k) = \frac{n}{\gcd(n,k)} = \frac{n}{1} = n$ اوپه نتیجه کې $< a^k > = G$

نوټ : د 5.7 لیما له مخې کولایی شوټول مولد *(generating)* عناصرد $(\mathbb{Z}_n\ ,+)$ ګروپ پیدا کړو. مثال په ډول $(\mathbb{Z}_{12}\ ,+)$ دورانی ګروپ دی چې $\mathbb{Z}_{12} =< \bar{5} >$ او ord($\mathbb{Z}_{12}$) = 12 دي.

$$\{k \in \mathbb{N} | \ 1 \le k \le 12 \ \wedge \ \gcd(12,k) = 1\} = \{ 1,5,7,11\}$$

څرنګه چې په دې مثال کې $a = \bar{5}$ دی. مونږ غواړو د 5.7 لیما د k = 7 لپاره تطبیق کړو

$$(\bar{5})^7 = \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} = \overline{35} = \overline{11} \Longrightarrow <\overline{11}> = \mathbb{Z}_{12}$$

همدارنګه $< \bar{7} > \ = \ < \bar{1} > = \mathbb{Z}_{12}$ صدق کوې

مثال: غواړو $M:=\{\bar{a} \in (\mathbb{Z}_5^*,.) \ | \ < \bar{a} > = \mathbb{Z}_5^*\}$ پیدا کړو.
به اسانی سره ثبوت کولاې چې $\mathbb{Z}_5^*$ یو دورانی ګروپ او $\mathbb{Z}_5^* = < \bar{3} >$ دی .

خرنګه چې $ord(\mathbb{Z}_5^*) = 4$ دی. پس:

$\{ k \in \mathbb{N} \mid 1 \le k \le 4 \;\wedge\; \gcd(4,k) = 1\} = \{ 1,3 \}$

خرنګه چې په دې مثال $a = \overline{3}$ ده. مونږ غواړو د 5.7 لیما د $k = 3$ لپاره تطبیق کړو

$(\overline{3})^3 = \overline{3}\,.\,\overline{3}\,.\,\overline{3} = \overline{27} = \overline{2}$

پس $< \overline{2} > = < \overline{3} > = \mathbb{Z}_5^*$ او $M = \{ \overline{2}, \overline{3} \}$

تمرین 5.4 :

(a) $\overline{M} := \{\bar{a} \in (\mathbb{Z}_{11}^*, .) \mid < \bar{a} > = \mathbb{Z}_{11}^* \}$ پیدا کړې

(b) $\overline{N} := \{\bar{a} \in (\mathbb{Z}_{14}, +) \mid < \bar{a} > = \mathbb{Z}_{14} \}$ پیدا کړې

لیما 5.8: دورانی (cyclic groups) ګروپونه تبدیلی ګروپونه دي .

ثبوت : که $(G, .)$ یو دورانی ګروپ وې . پس باید یو $a \in G$ وجود ولری چې $< a > = G$ شي

$$x, y \in < a > \Longrightarrow \exists\, m, n \in \mathbb{N}\,; x = a^m \;\wedge\; y = a^n$$
$$\Longrightarrow x.y = a^m.a^n = a^{m+n} = a^{n+m}$$
$$= a^n.a^m = y.x$$
$$\Longrightarrow G \; commutative$$

تعریف 5.2: د $n \in \mathbb{N}$ لپاره لاندې تابع Euler – function په نوم یادیږي

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \longmapsto \varphi(n) = |\{k \in \mathbb{N} \mid 1 \le k \le n \;\wedge \gcd(n,k) = 1\}|$$

یعنې $\varphi(n)$ مساوی دهغو ټول k شمیردی چې $1 \le k \le n$ او $\gcd(n,k) = 1$ وې . د مثال په ډول

n =1

$\varphi(1) = |\{k \in \mathbb{N} \mid 1 \le k \le 1 \;\wedge \gcd(1,k) = 1\}|$
$= |\{1\}| = 1$

n =2

$\varphi(2) = |\{k \in \mathbb{N} \mid 1 \le k \le 2 \;\wedge \gcd(2,k) = 1\}|$
$= |\{1\}| = 1$

n =3

$\varphi(3) = |\{k \in \mathbb{N} \mid 1 \le k \le 3 \;\wedge \gcd(3,k) = 1\}|$
$= |\{1,2\}| = 2$

n =4

$\varphi(4) = |\{k \in \mathbb{N} \mid 1 \le k \le 4 \;\wedge \gcd(4,k) = 1\}|$
$= |\{1,3\}| = 2$

n =5

$\varphi(5) = |\{k \in \mathbb{N} \mid 1 \le k \le 5 \ \wedge \gcd(5,k) = 1\}|$
$= |\{1,2,3,4\}| = 4$
n= 6
$\varphi(6) = |\{k \in \mathbb{N} \mid 1 \le k \le 6 \ \wedge \gcd(6,k) = 1\}| = |\{1,5\}| = 2$
n =7
$\varphi(7) = |\{k \in \mathbb{N} \mid 1 \le k \le 7 \ \wedge \gcd(7,k) = 1\}|$
$= |\{1,2,3,4,5,6\}| = 6$
n= 8
$\varphi(8) = |\{k \in \mathbb{N} \mid 1 \le k \le 8 \ \wedge \gcd(8,k) = 1\}|$
$= |\{1,3,5,7\}| = 4$

لیدل کیږي ، که p یولمړنی (اولیه) عدد وی. بیا:

$$\varphi(p) = |\{k \in \mathbb{N} \mid 1 \le k \le p-1\}| = p-1$$

ځکه د ټولو $1 \le k \le p-1$ لپاره gcd(k,p) = 1 رابطه صدق کوي

لیما 5.9 : که مرتبه (order) دیو G دورانی ګروپ n وي. بیا دهغو عناصرو شمیرچي مولد (generator) د G دي ، مساوي $\varphi(n)$ دی .

ثبوت : ثبوت د 5.7 لیما اود $\varphi(n)$ (Euler function) تعریف څخه لاسته راځی .

د مثال په ډول په $(\mathbb{Z}_{10}\ , +)$ دورانی ګروپ کي د مولد (generator) عناصرو شمیر 4 دی. ځکه:

n= 10
$\varphi(10) = |\{k \in \mathbb{N} \mid 1 \le k \le 10 \ \wedge \gcd(8,k) = 1\}|$
$= |\{1,3,7,9\}| = 4$

که p یولمړنی (اولیه) عدد وي. بیا د مولدو (generator) عناصروشمیرپه $(\mathbb{Z}_p\ , +)$ کي $\varphi(p) = p-1$ دی .د مثال په ډول مونږ د $(\mathbb{Z}_5\ , +)$ ګروپ په نظرکي نیسو. 5 یو لمړنی عدد دی. پس باید 4 = 1- 5 = $\varphi(5)$ وي

$\varphi(5) = |\{1,2,3,4\}| = 4$
$\mathbb{Z}_5 = <\bar{1}> = <\bar{2}> = <\bar{3}> = <\bar{4}>$

نوټ: د $(\mathbb{Z}_5^*, .)$ ګروپ مرتبه مساوی 4 او φ یوه Euler function ده
$\varphi(4) = |\{1,3\}| = 2$

لیما 5.9 یوازي شمیر د مولدوعناصرو معلومه وي. په پورتنی مثال کي:

$<\bar{2}> = <\bar{3}\ge = (\mathbb{Z}_5^*, .)\quad , \quad <\bar{1}> \ne \mathbb{Z}_5^*$

تمرین 5.5: د *Euler function* څخه استفاده وکړی او دالاندي m اوn اعداد پیداکړی

(a) m:= | $\{\bar{a} \in (\mathbb{Z}_{16}, +) \mid < \bar{a} > = \mathbb{Z}_{16}\}$ |

(b) n:= | $\{\bar{a} \in (\mathbb{Z}_7^*, .) \mid < \bar{a} > = \mathbb{Z}_7^*\}$ |

تعريف 5.3 :

$\mathbb{Z}_n^{\mathrm{x}} := \{\bar{a} \in \mathbb{Z}_n \mid \bar{a} : invertible$ (معکوس قبلونکی)}

$(\mathbb{Z}_n^{\mathrm{x}}, .)$يو ګروپ دی او د *prime residue class group* په نوم یادیږي.

ليما 5.10: $n \in \mathbb{N}$ او φ يوه *Euler function* ده . بيا :

$(\mathbf{a})\ \mathbb{Z}_n^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_n \mid \gcd(n,k) = 1\}$

(b) $|\mathbb{Z}_n^{\mathrm{x}}| = \varphi(n)$

ثبوت (a) :

$$\bar{k} \in \mathbb{Z}_n^{\mathrm{x}} \Longrightarrow \exists \bar{r} \in \mathbb{Z}_n ;\ \bar{1} = \bar{k}.\bar{r} = \overline{k.r}$$

$$\Longrightarrow 1 - kr \in n\mathbb{Z}$$ [د 5.12 ليما له مخې]

$$\Longrightarrow \exists s \in \mathbb{Z} ; 1 - \mathrm{kr} = \mathrm{sn}$$

$$\Longrightarrow 1 = rk + sn \Longrightarrow \gcd(n,k) = 1$$

$$\Longrightarrow \mathbb{Z}_n^{\mathrm{x}} \subseteq \{\bar{k} \in \mathbb{Z}_n \mid \gcd(n,k) = 1\}$$

له بلې خوا:

$$k \in \mathbb{Z} ;\ \gcd(\mathrm{n,k}) = 1$$

$$\Longrightarrow \exists\, r, s \in \mathbb{Z} ; \mathrm{r.k} + \mathrm{s.n} = 1$$

$$\Longrightarrow \bar{1} = \overline{r.k + s.n} = \bar{r}\,.\bar{k} + \bar{s}\,.\bar{n}$$

$$= \bar{r}\,.\bar{k} + \bar{s}\,.\bar{0} = \bar{r}\,.\bar{k}$$

$$\Longrightarrow \bar{k}\ invertible \Longrightarrow \bar{k} \in \mathbb{Z}_n^{\mathrm{x}}$$

په نتيجه کې : $\mathbb{Z}_n^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_n \mid \gcd(n,k) = 1\}$

د (b) ثبوت د φ *Euler function* څخه لا سته راځي .

مثال: د 5.10 ليما له مخې لاندې ګروپونه prime residue class group دي:

$$\mathbb{Z}_1^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_1 \mid \gcd(1,k) = 1\} = \{\bar{1}\}$$

$$\mathbb{Z}_2^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_2 \mid \gcd(2,k) = 1\} = \{\bar{1}\}$$

$$\mathbb{Z}_3^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_3 \mid \gcd(3,k) = 1\} = \{\bar{1}, \bar{2}\}$$

$$\mathbb{Z}_4^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_4 \mid \gcd(4,k) = 1\} = \{\bar{1}, \bar{3}\}$$

$$\mathbb{Z}_5^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_5 \mid \gcd(5,k) = 1\} = \{\bar{1}, \bar{2}, \bar{3}\}$$

تمرين 5.6: د 5.10 ليما له مخې لاندې prime residue class ګروپونه پيدا کړئ:

$(\mathbb{Z}_{16}^{\mathrm{x}}, .)$, $(\mathbb{Z}_{20}^{\mathrm{x}}, .)$ او $(\mathbb{Z}_{36}^{\mathrm{x}}, .)$

شپږم فصل

حلقه (Ring)

تعریف 6.1 : یو الجبری جوړښت $(R, \oplus\ , \odot)$ د لاندي خواصو سره د حلقی (Ring) په نوم یادیږي.

(1) $(R, \oplus)$ یو تبدیلی گروپ (commutative group) دی.

(2) اتحادی (associative) نظر "$\odot$" : یعني

$$(a\odot b)\odot c = a\odot(b\odot c) \qquad (\forall a, b, c \in R\ )$$

(3) توزیعی (distributive) نظر $\oplus$-$\odot$: یعني

$\forall a, b, c \in R$

$$a\odot(b\oplus c) = (a\odot b)\oplus(a\odot c)$$

$$\wedge$$

$$(b\oplus c)\odot a = (b\odot a)\oplus(c\odot a)$$

که یو رینگ نظر "$\odot$" ته عینیت (identity) عنصرولرې د Ring with identity په نوم یادیږي. یعني

$$\exists I_R \in R;\ a\odot I_R = a \qquad (\ \forall a \in R\ \ )$$

عینیت عنصر نظر "$\odot$" د واحد (unity) په نوم یادیږي

که R نظر "$\odot$" ته تبدیلی وی. ورته تبدیلی رینگ (commutative) ویل کیږي. یعني که:

$$a\odot b = b\odot a \qquad (\ \forall a, b \in\ R\ )$$

مثال: $(\mathbb{R}, +, .), (\mathbb{Q}, +, .), (\mathbb{Z}, +, .)$ تبدیلی رینگونه دي چې دهغوي واحد (unity) عنصر یو "1" دی. همدارنگه $(\ \mathbb{Z}_n, +,\ \ .\ )$ یو تبدیلی رینگ چې واحد عنصریې $\bar{1}$ دی.

نوټ: مونږبه پس له دي د $(R, \oplus\ , \odot)$ پرځای (R,+,.) لیکو. په دي شرط چې غلط فهمی ونشي. نظر " $\oplus$ " ته د عینیت عنصرپه "0" او معکوس د a په -a سره ښیو. نظر "$\odot$" ته واحد عنصر په "1" اومعکوس د a په a^{-1} سره ښیو.

مثال 6.1 : $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ نظر لاندي دوه گوني رابطي (Binary operation) ته چې په جدول کې ښودل شوې ده یو Ring (حلقه) دی .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

مثال 6.2 : R=(0,1,2)

پر R باندي دا لاندي دوه ګوني رابطه (binary operation) تعريف شوې ده

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

په آساني سره کولای شو ثبوت کړوچې (. , + ,R) يوه Ring (حلقه) ده .
مګر واحد عنصر نه لری

تمرين 6.1: $M:= \{ \ A \in M(2x2, \mathbb{R}) \,|\, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \}$

ثبوت کړی چې (.,+,M) يوه حلقه (Ring) ده. البته دلته دوه ګوني رابطي د
متريکسو جمع او ضرب دي .

تمرین 6.2:

S:= $\{2x+1 \mid x \in \mathbb{Z}\}$, R:= $\{ 2x \mid x \in \mathbb{Z} \}$

ایا (R,+,.) او (S,+,.) رینگونه دي

لیما 6.1 : (R,+,.) یو رینګ دی. د $a \in R$ لپاره دا لاندي تابع یوه G- End ده.

$$\rho_a : (R,+) \longrightarrow (R,+)$$
$$x \longmapsto a.x$$

ثبوت:

$x, y \in R, \rho_a(x+y) = a.(x+y) =$ a.x + a.y
$= \rho_a(x) + \rho_a(y)$

قضیه 6.1 **:** (R,+,.) یو رینګ او صفر ("0") یی د عینیت عنصر نظر "+" ته دی. د $a, b, c \in R$ لپاره دالاندي افادي صدق کوي.

(1) 0 = 0.a = a. 0

(2) a.(-b) = (-a).b = -(a.b)

(3) (-a).(-b) = a.b

(4) a.(b-c) = (a.b) - (a.c)

(1) ثبوت :

(a . 0) + 0 = a.0 = a.(0+0) [توزیعی خاصیت]
= (a.0) + (a.0)
$\Longrightarrow a.0 = 0$ [د 1.2 قضیی له مخې]

په همدې ډول ثبوت کیدای شي چې 0.a = 0 کیږي.

ثبوت (2) :

0 = 0.b = (a +(-a)).b =a.b + (-a).b

پس لهذا b.(a-) معکوس (inverse) د (a.b) دی. یعني a. b = (-a).b

ثبوت (**3**) : د ثبوت لپاره د ρ_a تابع (لیما 6.1) څخه استفاده کو :

$(-a).(-b) = \rho_{-a}(-b) = -\left(\rho_{-a}(b)\right)$
$= -(\ -a\,.\,b) = a.b$

ثبوت (**4**) **:** دلته هم د $\boldsymbol{\rho_a}$ څخه استفاده کو:

$\rho_a: (R, +) \longrightarrow (R, +)$
$b - c \longmapsto a.(b - c)$
a.(b –c) = $\rho_a(b - c)$
$= \rho_a b - \rho_a c$ [G-Hom یو"+" نظر ρ_a ځکه]
$= (a.b) - (a.c)$

تعریف 6.2 : (.,+,R) رینګ د واحد (unity) عنصرسره دی. یو a ∈ R ته unit او یا invertible ویل کیږی، که چیري په R کې d,c د لاندي خواصو سره موجود وي:

$$c.a=1 \quad \wedge \quad a.d=1$$

یعني a نظر "." ته چپ او ښي معکوس پذیر وي.

مثال

(a) د $(\mathbb{Z}, +, .)$ په رینګ کي یوازې 1- او 1 معکوس پذیر(invertible) دي .

(b) $(\mathbb{Q}, +, .)$ په رینګ کې غیرله صفر څخه نورټول عناصریی Unit یعني معکوس پذیر دي.

(c) د $(2\mathbb{Z}, +, .)$ رینګ هیچ معکوس پذیر(invertible) نه لري. ځکه واحد (unity) عنصر نه لري.

(d) په $(\mathbb{Z}_6, +, .)$ رینګ کي معکوس پذیر (invertible) $\overline{1}$ او $\overline{5}$ دي. مګر په $(\mathbb{Z}_5, +, .)$ معکوس پذیر $\overline{1}$ ، $\overline{2}$، $\overline{3}$ او 4 دي

قضیه 6.2 : (.,+,R) یو رینګ د واحد (unity) عنصرسره دی. که R_u په R کې سیټ د ټولو معکوس پذیر (invertible) عناصروي. بیا :

$\boldsymbol{a} \in R_u, b \in R, (b.a = 1 \vee a.b = 1) \Rightarrow b \in R_u$ (1)

(2) $(R_u , .)$ یو ګروپ دی.

ثبوت (1) :

$a \in R_u \Rightarrow \exists c \in R; a.c = 1$ فرض کوچې b.a = 1 صدق کوې. بیا :

$b = b.1 = b.(a.c) = (b.a).c = 1.c = c$
$\Rightarrow$ a.b = a.c
$\Rightarrow b.a = 1 = a.c = a.b \Rightarrow b \in R_u$

ثبوت(2) :

دوه ګوني رابطه : باید ثبوت شي چې د $a, a' \in R_u$ لپاره باید $a.a' \in R_u$ وی.

$a, a' \in R_u$

$\Rightarrow \exists b, b', c, c' \in R; b.a = a.c = 1 \quad \wedge \quad b'.a' = a'.c' = 1$

(a.a’).(c’. c) = a.(a’.c’).c = a.1.c=a.c =1

(b’.b).(a.a’) = b’.(b.a).a’ = b’.1.a’=b’.a’=1

$\Rightarrow a.a' \in R_u$

$1.1 = 1 \Rightarrow 1 \in R_u$

$\forall a \in R_u, \exists b \in R; a.b = 1 \Rightarrow b \in R_u$ [د (1) له مخې]
په دې معنی چې b نظر ”.“ ته معکوس د a دی.

تعریف 6.3 : (R,+,.) یو رینګ او R ⊇ $\bar{R}$ ≠ ϕ . $\bar{R}$ د فرعی رینګ (subring) په نوم یادیږي، که چیرې $(\bar{R}, +, .)$ یو رینګ وي.

لیما 6.2 : (R,+,.) یو رینګ، $\phi \neq S \subseteq R$. بیا دالاندي افادی دیوبل سره معادل دي:

(a) S یو فرعی رینګ (Subring) د R دی.

(b) د هر $x, y \in S$ لپاره لرو:

(i) $x - y \in S$

(ii) $x.y \in S$

ثبوت $(\boldsymbol{a}) \Rightarrow (\boldsymbol{b})$: ځرنګه چې هر فرعی رینګ په خپله رینګ هم دی.
پس $(S, +, .)$ هم یو رینګ دی. پس $(S, +)$ یو فرعی ګروپ د (R,+) دی.

د 3.2 قضیی له مخې $(\boldsymbol{i})$ صدق کوي. $(\boldsymbol{ii})$ هم صدق کوي. ځکه S د فرعی رینګ په حیث دا خواص لري .

ثبوت $(\boldsymbol{b}) \Rightarrow (\boldsymbol{a})$ **:** د **(i)** څخه نتیجه اخلو چې $(S, +)$ د 3.2 قضیی په اساس یو فرعي ګروپ د (R,+) دی .
د $(\boldsymbol{ii})$ څخه نتیجه اخلو چې ”.“عملیه پر S قابل د تطبیق ده.ځرنګه چې اتحادی (Associative) او توزیعی (Distributive) خواص په R کې صدق کوي، پس په S کې هم صدق کوي. په نتیجه کې $(S, +, .)$ یو فرعی رینګ د R دی.

مثال:

(a) $(\mathbb{Q}, +, .), (\mathbb{Z}, +, .)$ فرعی رینګونه د $(\mathbb{R}, +, .)$ دي.

(b) $(\mathbf{2}\mathbb{Z}, +, .)$ یو فرعی رینګ د $(\mathbb{Z}, +, .)$ دی . بدون د واحد عنصر „ 1 “

(c) که $(R, +, .)$ یو رینګ وي، په خپله R او {0} فرعی رینګونه د هغه دي

(d) $M(nxn, \mathbb{Z})$ یو فرعی رینګ د $M(nxn, \mathbb{R})$ دی.

مثال 6 .3 :

(a) **د** S سیت په لاندي ډول تعریف شوی دی:

$$S:=\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

S یو فرعی رینګ د $M(2x2, \mathbb{R})$ دی ، چې واحد عنصریی دالاندي متریکس دی

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

د S واحد عنصرخلاف د $M(2x2, \mathbb{R})$ **د** واحد عنصر دی . یعني

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(b)

$$\mathrm{M}:= \{A \in M(2x2, \mathbb{R}) \}, \mathrm{S}:= \{A \in M(2x2, \mathbb{R}) \,|\, A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \}$$

S یو subring په (M,+,.) کې دی. ځکه:

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \mathrm{B} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in \mathrm{S}$$

$$\mathrm{A} - \mathrm{B} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ -b+d & a-c \end{pmatrix} \in S$$

$$\mathrm{A.B} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} . \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} \in \mathrm{S}$$

د 6.2 لیما له مخې S یو subring په (M,+,.) کې دی.

تعریف 6.4 : $(R,+,.)$ یو رینګ دی او I یو فرعي ګروپ د (R,+) دی.

د left-ideal په نوم یادیږي ، که چیري :

$$\forall r \in R, \forall a \in I \Rightarrow r.a \in I \qquad (\text{یعني} \quad I.R \subseteq I)$$

I د right-ideal په نوم یادیږي، که :

$$\forall r \in R, \forall a \in I \Rightarrow a.r \in I \qquad (\text{یعني} \quad I.R \subseteq I)$$

I ته ideal ویل کیږي که I یو left-ideal او right-ideal وی .

مثال 6. 4 : مونږپوهیږو چې $\mathrm{R}:=\mathrm{M}(2\mathrm{x}2, \mathbb{Q})$ نظر ضرب اوجمع د متریکس یو رینګ دی. یعني :

(a)   (R,+) یو تبدیلی گروپ (commutative) دی .

(b) $\forall A, B \in R \ \Rightarrow A.B \in R$

(c)   د رینگ نورخواص هم صدق کوي .

د متریکس عینت صفرمتریکس او واحد عنصر یی واحد متریکس دی. یعني:

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

اوس د $\boldsymbol{L}$ سیت په لاندي شکل تعریفو :

$$L := \left\{ \begin{pmatrix} 0 & p \\ 0 & q \end{pmatrix} \mid p, q \in \mathbb{Q} \right\}$$

L یو Left ideal د $\mathbb{Q}$, R=M(2x2) **)** دی . ځکه :

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in L$$

$$A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}, \ B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} \in L$$

$$\Rightarrow \ A + B = \begin{pmatrix} 0 & a + c \\ 0 & b + d \end{pmatrix} \in L$$

$$-A = \begin{pmatrix} 0 & -a \\ 0 & -b \end{pmatrix} \in L$$

پس (L,+) د 3.1 قضیی له مخې یو فرعی گروپ د (R,+) دی.

علاوه پر هغه **:**

$$D = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M(2x2, \mathbb{Q})$$

$$D \,.\, A = \begin{pmatrix} x & y \\ z & t \end{pmatrix} . \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & xp + yt \\ 0 & zp + tq \end{pmatrix} \in L$$

پس L یو Left ideal په M(2x2, $\mathbb{Q}$) کې دی .

تمرین 6.3 **:** د $S \subseteq \boldsymbol{R}$ (R د 6.4 مثال رینگ دی) سیت په لاندي ډول تعریف شوی ده:

$$S := \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in \mathbb{Q} \right\}$$

ثبوت کړی چې S یو Subring (فرعی رینگ) د R دی.

تمرين 6.4:

M:= $\{ A \in M(2x2, \mathbb{R}) \mid A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a^2 + b^2 \neq 0 \}$

ايا (M,+,.) نظرجمع "+" او ضرب "." متريكس ته رينګ دی

قضيه 6.3 : $(R,+,.)$ يو رينګ د واحد „ 1" عنصرسره او $\boldsymbol{I} \subseteq \boldsymbol{R}$. بيا:

$$\left.\begin{array}{l}(1) I \neq \phi \\ (2) a, b \in I \Rightarrow a+b \in I \\ (3) r \in R, a \in I \Rightarrow r.a \in I\end{array}\right\} \Longleftrightarrow I \text{ يک ايديال}$$

ثبوت: " $\Leftarrow$ " د ايديال تعريف له مخې واضح ده.

ثبوت" $\Rightarrow$ "**:** که $\boldsymbol{I} = \{0\}$ وې. بيا واضح ده چې $\boldsymbol{I}$ يو ايديال دی.

که $\boldsymbol{I} \neq \{0\}$ وې. بيا:

$I \neq \phi \ \wedge \ I \neq \{0\} \quad \Longrightarrow \exists a \in I \ , a \neq 0$

$0 \in R, a \in I \Rightarrow 0.a = 0 \in I$ [د (3)]

$a \in I \Rightarrow -a = -(1.a) = -1.a$

$\Rightarrow -\boldsymbol{a} \in \boldsymbol{I}$

$\forall \ a, b \in I \Rightarrow a + b \in I$ [(2)]

$\Rightarrow (I, +)$ is Subgroup (فرعي ګروپ) [قضيه 3.1]

$\Rightarrow$ I is a ideal [(3)]

مثال:

(a) (R,+,.) يو رينګ دی. {0} (Zero-ideal) او R خپله ايديال دی.

(b) په $(\mathbb{Z}, +, .)$ رينګ کې د $(\boldsymbol{n}\mathbb{Z}, +)$ فرعی ګروپ يوايديال دی. ځکه:

$$\forall \ z \in \mathbb{Z}, nz \in n\mathbb{Z} \Rightarrow nz.z = n(z.z) \in n\mathbb{Z}$$

(c) $(\mathbb{Z}, +, .)$ يو فرعی رينګ د $(\mathbb{Q}, +, .)$ دی، مګر ايديال نه دی. ځکه:

$$\frac{1}{2} \in \mathbb{Q}, 1 \in \mathbb{Z}, \ \frac{1}{2}.1 = \frac{1}{2} \notin \mathbb{Z}$$

ليما 6.3: (R,+,.) يو رينګ دي

(1) (I_i) ايديال په R کې دي، $J := \{1, \dots, n\}$. که $I := \bigcap_{i \in J} I_i$ وي، بيا I هم يو ايديال دی

(2) I يو اديال او S يو فرعی رينګ په R کی دی. بيا:

(a) دالاندي سیت یو فرعی رینگ په R کی دی
$S + I = \{ x+y \mid x \in S , y \in I \}$
(b) S ∩ I یو ادیال په S کی دی
ثبوت: I د 3.11 لیما له مخې یو فرعی گروپ په (R,+) کې دی.

$a \epsilon I ,\ r \epsilon R \ \Rightarrow\ a\ \epsilon I_i \quad (\forall\ i \epsilon J)$
$\qquad \Rightarrow r.a\ \epsilon I_i \quad (\forall\ i \epsilon J)$ [ځکه I_i ایدیال دي]
$\qquad \Rightarrow r.a\ \epsilon I$

په نتیجه کې I هم یو ایدیال دی .
ثبوت(2):
(a)

u, w∈ S+I
$\Rightarrow\ \exists\ u_1, w_1 \in S\ \wedge\ \exists\ u_2, w_2 \in I\ ;\ u = u_1 + u_2\ ,\ w = w_1 + w_2$
$\Rightarrow\ u - w = (u_1 - w_1) + (u_2 - w_2) \in S+I$
$u.w = (u_1 + u_2) . (w_1 + w_2)$
$\quad = u_1 . w_1 + (u_2 . w_1 + u_1 . w_2 + u_2 . w_2)$
$u_1 . w_1 \in S$ [ځکه S فرعی رینگ]
$u_2 . w_1 + u_1 . w_2 + u_2 . w_2 \in I$ [ځکه I ادیال]
په نتیجه کی u. w∈ S+I او S+I د 6.2 لیما له مخې فرعی رینگ است
ثبوت(b):

$w \in S \cap I\ \Rightarrow\ \exists\ a \in S\ \wedge\ \exists\ b \in I\ ;\ w = a\ ,\ w = b$
$\qquad \Rightarrow w.x = a.x = b.x \quad (\forall\ x \in S)$
$\qquad \Rightarrow w.x = a.x \in S\ \wedge\ w.x = b.x \in I$
$\qquad \Rightarrow w.x \in S \cap I$

په نتجه کي S ∩ I یو ادیال د S دی.
تعریف 6.5 : **(R,+,.)** او (S,+,.) دوه رینگه دي . $\varphi: R \to S$ د

Ring homomorphism (R- Hom) په نوم یادیږي. په دې شرط چې د هر $a, b \in R$ لپاره لاندي افادي صدق وکړي

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\wedge$$

$$\varphi(a.b) = \varphi(a).\varphi(b)$$

نوت: په ځینو کتابوکی د رینگ هومومورفیزم په تعریف کی لاندي شرط هم علاوه کوی

$$\boldsymbol{\varphi(1_R) = 1_s}$$

مګرمونږ دلته دپورتنی شرط څخه صرف نظر کوو

که R-Hom یو injective وي، د Ring Monomorphism

(R-Monom) په نوم، که surjective وي د Ring Epimorphism (R-Epim) اوکه bijective وي د Ring Isomorphism (R-Isom) په نوم یادیږي .

یو R-Hom د Ring Endomorphism (R-Endo) په نوم یادیږي که چیري S = R وي . یو R-Endo چې په عین وخت کی bijective وي ، د Ring Automorphism (G-Auto) په نوم یادیږي .

که د R اوS رینګو عینت عناصر 0_R و $\mathbf{0_s}$ وي، بیا:

$$\varphi(0_R) = 0_s$$

ځکه:

$$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R) \Longrightarrow \varphi(0_R) = 0_s$$

مثال 6.5 : پوهیږوچې $(\mathbb{C}, +, .)$ یو رینګ دی. اوس ښیوچې دالاندي تابع یو R-Hom ده

$$\varphi: (\mathbb{C}, +, .) \to (\mathbb{C}, +, .)$$
$$\boldsymbol{z = (x + iy) \mapsto \bar{Z} = (x - iy)}$$

حل:

$$z = x + iy \;, z_1 = x_1 + iy_1 \in \mathbb{C}$$

2.1 مثال کې موولیدل چې φ نظر "+" ته یو G-Hom دی. یعني

$$\varphi(z + z_1) = \varphi(z) + \varphi(z_1)$$

له بلې خوا:

$$\varphi(z.z_1) = \varphi\big((x + iy).(x_1 + iy_1)\big)$$
$$= \varphi(xx_1 + iyx_1 + ixy_1 - yy_1)$$
$$= \varphi(xx_1 - yy_1 + (yx_1 + xy_1)i)$$
$$= xx_1 - yy_1) - (yx_1 + xy_1)i$$

$$\varphi(z).\varphi(z_1) = (x - iy).(x_1 - iy_1)$$
$$= xx_1 - iyx_1 - ixy_1 - yy_1$$
$$= (xx_1 - yy_1) - (yx_1 + xy_1)i$$

په نتيجه کې $\varphi(z.z_1) = \varphi(z).\varphi(z_1)$

مثال 6.6 : پر $(\mathbb{Z}_2,+,\ .\ )$ رينګ بانه دي دا لاندي تابع تعريف شويده:

$$\boldsymbol{\varphi}: \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$$
$$\bar{x} \longmapsto \bar{x}\ .\ \bar{x} = (\bar{x})^2$$

φ يو R-Hom دی. ځکه:

$\bar{x}, \bar{y} \in \mathbb{Z}_2$

$$\varphi(\bar{x}+\bar{y}) = (\bar{x}+\bar{y})^2 = (\bar{x})^2 + \bar{x}.\bar{y} + \bar{x}.\bar{y} + (\bar{y})^2$$

د $\bar{x}.\bar{y}$ لپاره دوه لاندي حالتونه امکان لري

لمړی حالت : $\bar{x}.\bar{y} = \bar{0}$

$$\varphi(\bar{x}+\bar{y}) = (\bar{x})^2 + (\bar{y})^2 = \bar{x}.\bar{x} + \bar{y}.\bar{y} = \varphi(\bar{x}) + \varphi(\bar{y})$$

دويم حالت : $\bar{x}.\bar{y} = \bar{1}$

$$\bar{x}.\bar{y} = \bar{1} \Rightarrow \bar{x} = \bar{1} \wedge \bar{y} = \bar{1}$$

$$\varphi(\bar{x}+\bar{y}) = (\bar{x})^2 + \bar{x}.\bar{y} + \bar{x}.\bar{y} + (\bar{y})^2$$
$$= (\bar{1})^2 + \bar{1}.\bar{1} + \bar{1}.\bar{1} + (\bar{1})^2 = \bar{4} = \bar{0}$$

$$\varphi(\bar{x}) + \varphi(\bar{y}) = (\bar{x})^2 + (\bar{y})^2$$
$$= \bar{1}.\bar{1} + \bar{1}.\bar{1} = \bar{1} + \bar{1} = \bar{2} = \bar{0}$$

په نتيجه کې

$$\varphi(\bar{x}+\bar{y}) = \bar{0} = \varphi(\bar{x}) + \varphi(\bar{y})$$

$$\varphi(\bar{x}.\bar{y}) = (\bar{x}.\bar{y})^2 = (\bar{y})^2\ .\ (\bar{x})^2$$

$$= (\bar{x})^2.(\bar{y})^2 \quad [\text{ځکه } \mathbb{Z}_2 \text{ تبديلی دی}]$$

$$= (\bar{x}).\varphi(\bar{y})$$

په نتيجه کې **φ** يو R-Hom دی.

تمرين 6. 5 : په $(\mathbb{Z},+,\ .\ )$ رينګ باندې لاندي تابع تعريف شوې ده:

$$\boldsymbol{\varphi}: \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$x \longmapsto 2x$$

ايا **φ** يو R-Hom دی

تمرين 6.6 : ايا پر $(\mathbb{Z}_3,+,\ .\ )$ رينګ باندي دا لاندي توابع R-Hom دي :

(a) $\varphi: \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$

$\bar{x} \longmapsto \bar{x}\ .\ \bar{x} = (\bar{x})^2$

(b) $\varphi: \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$

$\bar{x} \longmapsto \bar{x}\ .\ \bar{x}\ .\ \bar{x} = (\bar{x})^3$

تمرين 6.7 :

(a) ثبوت کړئ چې دا لاندي تابع يوه R-Aut ده

$$\varphi: (\mathbb{C},+,.) \to (\mathbb{C},+,.)$$
$$z = (x+iy) \mapsto (x-iy)$$

(b) ثبوت کړئ چې دالاندي تابع يوه R-Isom ده

$$\mathrm{R} := \{A \in M(2x2,\mathbb{R}) \,|\, A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\}$$

$$\varphi: (\mathbb{C},+,.) \longrightarrow \mathrm{R}$$
$$z = a+ib \longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

تمرين 6.8 : (R,+,.) يو رينګ ، "1" يي واحد (unity) عنصر او $a \in R$ يومعکوس پذير **(invertible)** عنصردی. ثبوت کړئ چې دالاندي تابع يوه **R-Aut** ده .

$$\mathrm{L_a} : \mathrm{R} \longrightarrow R$$
$$x \longmapsto a\,x\,a^{-1}$$

تعريف 6.6 : (R,+,.) يو رينګ دی. يو ايديال I د Prime Ideal په نوم ياديږي که چيرې:

(i) $I \neq R$

(ii) $\forall x, y \in R\ ,\ x.y \in I \Rightarrow x \in I\ \ \vee\ \ y \in I$

مثال:

(a) په $(\mathbb{Z}\ ,+,.)$ رينګ کی د $p\mathbb{Z}$ سيت يو Prime Ideal دی، پدی شرط چه P يولمړنی عدد وي

حل: $p\mathbb{Z} \neq \mathbb{Z}$ دی. ځکه دمثال په ډول p=3 لپاره 4 په $p\mathbb{Z}$ شامل ندی .

له بلی خوا:

$$a,b \in \mathbb{Z}\ , a.b \in p\,\mathbb{Z} \Rightarrow p\,|\,a.b \Rightarrow p\,|\,a\ \ \vee\ \ p\,|\,b$$
$$\Rightarrow a \in p\,\mathbb{Z}\ \ \vee\ \ b \in p\,\mathbb{Z}$$

په نتيجه کی $p\mathbb{Z}$ يو prime ideal دی

په (.,+, ℤ) رینګ کی د p2ℤ سیت یو Prime Ideal دی. په (.,+, 2ℤ)
رینګ کي د 4ℤ ادیال یوپرایم ادیال نه دی. ځکه:

$2 \in 2\mathbb{Z} \quad \Rightarrow \quad 2.2 = 4 \in 4\mathbb{Z}$

مګر $2 \notin 4\mathbb{Z}$

قضیه 6.4 : که (.,+,R) او (.,+,S) دوه رینګه او $\varphi: R \to S$ یو R-Hom
وي . بیا :

(a) $\ker\varphi$ یو ایدیال په R کې دی .

(b) $\varphi(R)$ یو *subring* (فرعی رینګ) په S کې دی .

(c) که φ یو surjective او I یو ایدیال په R کې وي. په دي صورت $\varphi(I)$
یو ایدیال په S کې دی .

ثبوت (a) : د 2.4 قضیی له مخې kerφ یو فرعی ګروپ په R کې نظر "+"
ته دی

$r\in R\ ,\ x \in \ker\varphi \ \Rightarrow\ \varphi(r.x) = \varphi(r).\ \varphi(x) = \varphi(r).0 = 0$
$\Rightarrow\ r.x \ \in \ker\varphi$

په نتیجه کې kerφ یو ادیال دی

ثبوت (b) : د 2.4 قضیی له مخې *Im(φ)* $= \varphi(R)$ یو فرعی ګروپ په S کې
نظر "+" دی.

$s_1, s_2 \in \varphi(R) \Rightarrow \exists r_1, r_2 \in R;\ \varphi(r_1) = s_1 \ \wedge\ \varphi\,(r_2) = s_2$

$\varphi(r_1.r_2) = \varphi(r_1).\varphi(r_2) = \ s_1.s_2$

$\Rightarrow s_1.s_2 \in \varphi(R)$

ولیدل شوچې د "." دوه ګونه رابطه *(Binary operation)* پر $\varphi(R)$ قابل د
تطبیق ده . پس په نتیجه کې $\varphi(R)$ یوه فرعی حلقه *(Subring)* د S دی .

ثبوت (c) : څرنګه چې I یو ایدیال دی , پس د ایدیال د تعریف له مخې یو فرعی
ګروپ په (R,+) هم دی او$\varphi(I)$ د 3.3 قضیی په اساس یوفرعی ګروپ د S
دی .

$b \in \varphi(I), s \in S$
$\Rightarrow \exists a \in I \ \wedge\ r \in R;$
$\varphi(a) = b\ , \varphi(r) = s$ [ځکه φ یو *Surjective* دی]

$r.a\in I$ [ځکه I یو ایدیال دی]

$$\Rightarrow s.b = \varphi(r).\varphi(a) = \varphi(ra) \in \varphi(I)$$

$$b.s = \varphi(a).\varphi(r) = \varphi(ar) \in \varphi(I)$$

نتیجه کې $\varphi(I)$ یو ایدیال په S دی .

قضیه 6.5 : (R,+,.) او (S,+,.) دوه رینګونه ، $I \subseteq S$ او S او $\varphi: R \to S$ یو R-hom دی. بیا:

I یو ایدیال په S کې $\Longleftarrow$ $\varphi^{-1}(I)$ یو ایدیال په R کې دی.

ثبوت:

$$r_1,r_2 \in \varphi^{-1}(I) \Rightarrow \varphi(r_1), \varphi(r_2) \in I$$
$$\Rightarrow \rho(r_1) + \varphi(r_2) = \varphi(r_1 + r_2) \in I$$
$$\Rightarrow r_1 + r_2 \in \varphi^{-1}(I)$$
$$r \in R, r_1 \in \varphi^{-1}(I)$$
$$\Rightarrow \varphi(r) \in S \ \wedge \ \varphi(r_1) \in I$$
$$\Rightarrow \varphi(r).\varphi(r_1) \in I \qquad [\text{ ځکه I ادیال دی }]$$
$$\Rightarrow \varphi(r.r_1) = \varphi(r).\varphi(r_1) \in I$$
$$\Rightarrow r.r_1 \in \varphi^{-1}(I)$$

په نتیجه کې $\varphi^{-1}(I)$ یو ایدیال په R کې دی.

تعریف 6.7: (R,+,.) یو رینګ او I یو ادیال په R کل دي. مونږ set (مجموعه) د I دټولو left-coset په R کې په R/I سره ښیو. یعنی:

$$R/I := \{ a + I \mid a \epsilon R \}$$

نظر په تعریف د رینګ (R,+) یو تبدیلی ګروپ (ablean group) دی او ادیال I یوفرعی نورمال ګروپ په R کې دی. $(R/I,+)$ د 3.18 قضیي له مخي نظر لاندي دوه ګونه رابطوته یو فکتور ګروپ (factor group) دی:

$$+ : R/I \ x\ R/I \longrightarrow R/I$$
$$(a + I , b + I) \longmapsto (a + I) + (a + I) = (a + b) + I$$

اوس "." دوه ګونه رابطه پر R/I باندي لاندي ډول تعریف کوو:

$$. : R/I \ x\ R/I \longrightarrow R/I$$
$$(a + I , b + I) \longmapsto (a + I).(a + I) = (a.b) + I$$

په نتیجه کي $(R/I,+,.)$ یو رینګ دی اود فکتوررینګ (factor ring) په نوم یادیږي.

مثال: مونږد $(\mathbb{Z}_6,+,.)$ رینګ په نظرکي نیسو، چه په هغه کي د **I** سیت په لاندي ډول تعریف شویدي:

$$\mathrm{I}:=\{\bar{0},\bar{2},\bar{4}\}$$

I یو ادیال په $\mathbb{Z}_6$ کي دی. ځکه:

لمړی: **I** یوفرعی ګروپ په $(\mathbb{Z}_6,+)$ دی .

دوم: دا لاندي رابطه هم صدق کوي:

$$\forall\ \bar{a}\in I\ \ \wedge\ \forall\ \bar{b}\in\mathbb{Z}_6\ \ \Longrightarrow\ \ \bar{a}.\bar{b}\ \in I$$

پس فکتوررینګ $(\mathbb{Z}_6/I,+,.)$ لاندي شکل لري:

$$\mathbb{Z}_6/I\ =\ \{\bar{a}+\mathrm{I}\mid \bar{a}\epsilon\mathbb{Z}_6\}=\{\mathrm{I},\{\bar{1},\bar{3},\bar{5}\}\}$$

که مونږ $\mathrm{H}:=\{\bar{1},\bar{3},\bar{5}\}$ ولیکو، پدي صورت :

$$\mathbb{Z}_6/I\ =\{\ \ \mathrm{I},\ \ \mathrm{H}\}$$

د "+" دوه ګوني رابطي له مخي عینیت عنصریي **I** او معکوس د **H** په خپله دي. ځکه:

$$\mathrm{I}+\mathrm{H}=\{\{\bar{0},\bar{2},\bar{4}\}+\ \{\bar{1},\bar{3},\bar{5}\}=\{\ \bar{0}+\bar{1},\bar{0}+\bar{3},\bar{0}+\bar{5},\bar{2}+\bar{1},$$
$$\bar{2}+\bar{3},\bar{2}+\bar{5}\ ,\ \ \bar{4}+\bar{1}\ ,\bar{4}+\bar{3}\ ,\bar{4}+\bar{5}\ \}$$
$$=\{\bar{1},\bar{3},\bar{5},\bar{3},\bar{5},\bar{1},\bar{5}\ ,\bar{2}\ ,\ \bar{3}\}=\{\bar{1},\bar{3},\bar{5}\}=\mathrm{H}$$
$$\mathrm{H}+\mathrm{H}=\{\{\bar{1},\bar{3},\bar{5}\}+\ \{\bar{1},\bar{3},\bar{5}\}$$
$$=\{\ \bar{1}+\bar{1},\ \bar{1}+\bar{3},\bar{1}+\bar{5},\bar{3}+\bar{1},\ \bar{3}+\bar{3},\ \bar{3}+\bar{5}\ ,$$
$$\bar{5}+\bar{1}\ ,\bar{5}+\bar{3}\ ,\ \bar{5}+\bar{5}\ \}$$
$$=\{\bar{2},\bar{4},\bar{0},\bar{4},\bar{0},\bar{2},\bar{0}\ ,\bar{2}\ \}=\ \ \{\ \bar{0},2,\bar{4}\}=\mathrm{I}$$

د ګروپ نور خواص هم صدق کوي. په نتیجه کي $(\mathbb{Z}_6/I\ ,+)$ یوتبدیلی ګروپ دی. پر $\mathbb{Z}_6/I$ باندي "**.**" دوه ګوني رابطه د $\bar{a},\bar{b}\in\mathbb{Z}_6$ لپاره په لاندي ډول تعریف شویده :

$$(\bar{a}+I\ ).\left(\bar{b}+I\ \right)=\left(\bar{a}.\bar{b}\right)+I$$

$\mathbb{Z}_6/I$ د "**.**" دوه ګوني رابطي له مخي الجبری جوړښت لري. دمثال په ډول:

$$\bar{a}=\ \bar{3}\ ,\bar{b}=\ \bar{5}\quad\Longrightarrow\ \ \bar{a}.\bar{b}+I=\bar{3}.\bar{5}+\{\ \bar{0},\bar{2},\bar{4}\}\ =\bar{3}+\{\ \bar{0},\bar{2},\bar{4}\}$$
$$=\{\ \bar{3},\bar{5},\bar{1}\ \}=H\in(\mathbb{Z}_6/I\ ,\ \ .)$$

دا دوه ګوني رابطه پر نورو عناصرهم صدق کوي. پس $(\mathbb{Z}_6/I\ ,+,.)$ فکتور رینګ دی

قضيه 6.5-A **(theorem of ring homomorphism) :**

که (R,+,.) ، (S,+,.) دوه رينګه او $\varphi: R \to S$ يو R-Hom وي، پدي صورت بيا د $R/\mathrm{Ker}\,\varphi$ او S ترمينځ يو R-Hom موجود دی چه $R/\mathrm{Ker}\,\varphi$ او $\varphi(R)$ سره ايزومورف دي. يعنی: $\varphi(R) \cong R/\mathrm{Ker}\,\varphi$

ثبوت:

د 4.6 قضيي له مخي $\mathrm{Ker}\,\varphi$ يو ايډيال دی او هغه په I ښيوو. پس R/I د 6.6-A تعريف له مخي يو فکتوررينګ دی

اوس دا لاندي تابع په نظرکي نيسو:

$$\psi:\ R/\mathrm{I} \longrightarrow \mathrm{S}$$
$$\mathrm{a}+I \ \longmapsto\ \varphi(a)$$

$$\psi\big((a+I)+(b+I)\big) = \psi\big((a+b)+I\big) \quad [\text{د } 3.18 \text{ قضيي له مخي}]$$
$$= \varphi(a+b)$$
$$= \varphi(a)+\varphi(b) \quad [\ \varphi \text{ يو R-Hom}\ ]$$
$$= \psi(\mathrm{a}+\mathrm{I}) + \psi(\mathrm{b}+\mathrm{I})$$

$$\psi\big((a+I).(b+I)\big) = \psi\big((a.b)+I\big) \quad [\text{د ".„ تعريف له مخي}]$$
$$= \varphi(a.b) = \varphi(a).\varphi(b)$$
$$= \psi(\mathrm{a}+\mathrm{I}).\ \psi(\mathrm{b}+\mathrm{I})$$

په نتيجه کي ψ يو R-Hom دی.

ψ injective :

$$\psi(a+I) = \psi(b+I)$$
$$\Longrightarrow\ \varphi(a) = \varphi(b) \Longrightarrow \varphi(a)-\varphi(b) = 0_s$$
$$\Longrightarrow \varphi(a-b) = 0_s \Longrightarrow a-b \in I \quad [\ \mathrm{I} = \ker\varphi \ \text{ځکه}\ ]$$
$$\Longrightarrow \mathrm{a}+\mathrm{I} = \mathrm{b}+\mathrm{I} \quad [\text{د } 3.11 \text{ قضيي له مخي}]$$
$\Longrightarrow \psi$ injective

له بلي خوا:

$$y \in \varphi(R) \subseteq S$$
$$\Longrightarrow\ \exists x \in R\,;\varphi(x) = y \ \Longrightarrow\ \psi(x+I) = \varphi(x) = y$$
$\Longrightarrow \psi:\ R/\mathrm{I} \longrightarrow \varphi(R)$ surjective

په نتيجه کي: $\varphi(R) \cong R/\mathrm{N}$

قضيه 6.5-B **(theorem of ring isomorphism) :**

که S فرعی رينګ او I ايډيال په (R,+,.) رينګ کي وي ، بيا:

(1) $S/S\cap\mathrm{I}$ او $(S+I)/\mathrm{I}$ فکتوررينګونه (factors-ring) دي

$(S+I)/\mathrm{I} \cong S/\mathrm{S}\cap\mathrm{I}$ **(2)**

(یعنی $S/\mathrm{S}\cap\mathrm{I}$ او $(S+I)/\mathrm{I}$ یوبل سره رینګ ایزومورف دي)

ثبوت (1): د 6.3 لیما له مخي پوهیږو:

$S+I$ یو فرعی رینګ په R ، $\mathrm{S}\cap\mathrm{I}$ ادیال په S او I ادیال په $S+I$ کي دي.

پس $S/\mathrm{S}\cap\mathrm{I}$ او $(S+I)/\mathrm{I}$) فکتوررینګ (ring-factors) دي

ثبوت (2): د 6.5-A قضیي له مخي لاندي تابع R-Hom ده:

$$\varphi: S \longrightarrow R/I$$
$$a \mapsto a+I$$
$$\varphi(S) = \{\, \mathrm{s}+\mathrm{I} \mid \mathrm{s}\in\mathrm{S}\,\}$$
$$= \{\,(\mathrm{s}+\mathrm{v})+\mathrm{I} \mid \mathrm{s}\in\mathrm{S}, \mathrm{v}\in\mathrm{I}\}$$ [3.11 نظر به قضیه]
$$= (S+I)/\mathrm{I}$$ [φ نظر به تعریف]

د 6.5-A قضیي له مخي لاندي تابع R-Isom ده:

$$\varphi^{-} : R/ker\varphi \longrightarrow \varphi(R)$$
$$\mathrm{a.ker}\varphi \longmapsto \varphi(a)$$

په (1) کي مولیدل چه $\mathrm{S}\cap\mathrm{I}$ ادیال په S کي دی. پس د 3.19 قضیه پر فرعی رینګ S هم صدق کوي. یعنی دالاندي تابع R -Isom ده

$$\varphi^{-} : S/\mathrm{S}\cap\mathrm{I} \to \varphi(S)$$
$$\mathrm{a.ker}\varphi \to \varphi(a)$$

څرنګه چه $\varphi(S) \cong S/\mathrm{S}\cap\mathrm{I}$ او $\varphi(S) = (S+I)/\mathrm{I}$ دي، پس په نتیجه کي:

$$(S+I)/\mathrm{I} \cong S/\mathrm{S}\cap\mathrm{I}$$

تعریف 6.8 : یوایدیال $\boldsymbol{I}$ په R رینګ کې د Principle Ideal په نوم یادیږي، که $\boldsymbol{I}$ یوازی یوعنصرولري.

تعریف 6.9 **:** (.,+, R) یو رینګ دی. $\boldsymbol{a}\in\boldsymbol{R}$ او $\boldsymbol{a}\neq\boldsymbol{0}$.

a د Left-zero-divisor (l.z.divisor) (د چپ قاسم صفر) په نوم یادیږي. که چیرې یو $\boldsymbol{b}\in\boldsymbol{R}$ ، $\boldsymbol{b}\neq\boldsymbol{0}$ موجود وې چې a.b=0 شې .

که b.a=0 . په دې صورت a ته یو Right-zero-divisor (r.z.divisor) (د ښي قاسم صفر) ویل کیږي. که a l.z.divisor او هم r.z.divisor وي. بیا هغه د zero divisor (قاسم صفر) په نوم یادیږي.

تعریف 6.10 : یو (.,+,R) رینګ د Ring without zero divisor په نوم یادیږی که چیري:

$$r_1, r_2 \in R\,, r_1.r_2 = 0 \Rightarrow r_1 = 0 \;\;\vee\;\; r_2 = 0$$

یعني بی له صفرڅخه بل هیڅ zero-divisor نشته .

قضيه 6.6 : $(R,+,.)$ و $(S,+,.)$ دوه رينګه د واحد (unity) سره دي . که $\boldsymbol{\varphi}: \boldsymbol{R} \to \boldsymbol{S}$ يو R-Hom او سورجکتيف (surjective) وي. بيا دالاندي افادي د يوبل سره معادل دي:

(1) S بی له zero-divisor (صفر قاسم) او $\mathbf{1} \neq \mathbf{0}$

(2) $Ker\varphi$ يو Prime ideal دی.

ثبوت "$(\mathbf{1}) \Rightarrow (\mathbf{2})$" **:**

$$x, y \in R, x.y \in Ker\varphi$$
$$\Rightarrow \varphi(x.y) = 0$$
$$\Rightarrow \varphi(x).\varphi(y) = \varphi(x.y) = 0$$
$$\Rightarrow \varphi(x) = 0 \ \vee \ \varphi(y) = 0 \quad [\text{ځکه S بدون قاسم صفر}]$$
$$\Rightarrow x \in Ker\,\varphi \ \vee \ y \in Ker\,\varphi \quad [\text{ځکه } \varphi \text{ يک prime Ideal}]$$

$$1 \in S \Rightarrow \exists r \in R, \varphi(r) = 1 \quad [\text{ځکه } \varphi \text{ يو سوريکتيف}]$$
$$\Rightarrow r \notin Ker\varphi \quad [\text{ځکه } 0 \neq 1]$$
$$\Rightarrow Ker\varphi \neq R$$

د 6.4 قضيی له مخي $Ker\varphi$ يو ايديال دی. پس ثبوت شو چې $Ker\varphi$ يو Prime ideal دی.

ثبوت "$(\mathbf{2}) \Rightarrow (\mathbf{1})$" **:** لمړی ښيو چې S بې له zero-divisor دی.

$$s_1, s_2 \in S, s_1.s_2 = 0$$
$$\Rightarrow \exists x, y \in R\ ;$$
$$s_1 = \varphi(x) \ \wedge \ s_2 = \varphi(y) \quad [\varphi \text{ سورجکتيف}]$$
$$\Rightarrow 0 = s_1.s_2 = \varphi(x).\varphi(y) = \varphi(x.y)$$
$$\Rightarrow x.y \in Ker\,\varphi$$
$$\Rightarrow x \in Ker\,\varphi \ \vee \ y \in Ker\,\varphi$$
$$\Rightarrow \varphi(x) = 0 \ \vee \ \varphi(y) = 0 \quad [Ker\varphi \text{ يو prime ideal}]$$
$$\Rightarrow s_1 = 0 \ \vee \ s_2 = 0$$

پس S بی له zero-divisor (قاسم صفر) دی.

اوس بايد ثبوت شي چې په S کې $\mathbf{1} \neq \mathbf{0}$ صدق کوي.

که 1= 0 وې . په دې صورت:

$$1 = \varphi(1) = 0 \Rightarrow 1 \in Ker\,\varphi$$

$$\Rightarrow R.1 = R \subseteq Ker\varphi \quad [\text{ځکه } Ker\varphi \text{ يو ايديال}]$$

له بلې خوا $Ker\ \varphi \subseteq R$ دی . پس په نتیجه کې $Ker\ \varphi = R$ کیږي. مګردا د Prime ideal تعریف سره تضاد دی. پس باید $1 \neq 0$ وې.

تعریف 6.11 : یو تبدیلي ring (R,+,.) چې واحد (unity) عنصریی "1" ، $\mathbf{1 \neq 0}$ او no-zero-divisor وې د Integral domain په نامه یادوي. یعنې باید:

$$r_1, r_2 \in R\ , r_1 . r_2 = 0 \ \ \Rightarrow r_1 = 0 \ \vee \ r_2 = 0$$

اویا

$$r_1, r_2 \in R\ , r_1 \neq 0 \ \wedge \ r_2 \neq 0 \Rightarrow \ \ r_1 . r_2 \neq \ 0$$

د مثال په ډول $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ او $(\mathbb{C}, +, .)$ اینتګرال دومین (integral domain) دي.

په 6.1 مثال کې موولیدل چې $(\mathbb{Z}_6, +, .)$ رینګ دی مګر integral domain ندی .ځکه $\bar{2}.\bar{3} = \bar{6} = \bar{0}$ مګر $\bar{2}$ او $\bar{3}$ خلاف د $\bar{0}$ ادي .

تعریف: لاندې سیټ د Gaussian integers په نوم یادیږي

$$\mathbb{Z}[i] = \{\, a + ib \ \big| \ a,b \in \ \mathbb{Z} \,\} \subset \mathbb{C}$$

مثال: $\mathbb{Z}[i]$ یو فرعی رینګ د $(\mathbb{C}, +, .)$ او integral domain هم دی

حل:

$a + ib, c+id \in \ \mathbb{Z}[i]$

$a + ib - (c+id) = (a-c) + i(b-d)$

$a - c\ , b-d \in \ \mathbb{Z} \ \Longrightarrow (a + ib) - (c+id) \in \ \mathbb{Z}[i]$

$(a + ib).(c+id) = ac + ibc + iad - bd = (ac - bd) + i(bc + ad)$

$(ac - bd)\ , (bc + ad) \in \ \mathbb{Z} \ \Longrightarrow (a + ib).(c+id) \in \ \mathbb{Z}[i]$

په نتیجه کې $\mathbb{Z}[i]$ د 6.2 لیما له مخې یوفرعی رینګ د $(\mathbb{C}, +, .)$ دی.

څرنګه چې $(\mathbb{C}, +, .)$ یو اینتګرال دومین دی، پس $\mathbb{Z}[i]$ هم دی.

مثال6.7 : $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ نظر "+" او "." ته چې په لاندې جدول کې تشریح شوې دي، یو رینګ دی .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$(\mathbb{Z}_5, +, .)$ يو تبديلي رينګ چې واحد (unity) عنصريی "$\bar{1}$" دی .
$\mathbb{Z}_5$ يو Integral domain هم دی . ځکه ($\mathbb{Z}_n^*$, .) د 3.22 قضيی په اساس يو ګروپ دی، په دي شرط چې n يو اوليه عدد وې.

$$\bar{b}, \bar{a} \in \mathbb{Z}_5 \ , \ \bar{a} \neq \bar{0} \quad \wedge \quad \bar{a} \,.\, \bar{b} = \bar{0}$$

$$\Rightarrow \bar{b} = \bar{1}.\, \bar{b} = (\bar{a})^{-1}.\bar{a} \,.\, \bar{b} = (\bar{a})^{-1} \,.\, \bar{0} = \bar{0}$$

$\Rightarrow \mathbb{Z}_5$ Integ-domain

مثال:($R:= M(2x2, \mathbb{R}$. پوهيږوچې (R,+,.) يورينګ دی.مګر اينتګرال دومين (integral domain) نه دی. ځکه:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in R$$

$$A.B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ليدل کيږي چې حاصل ضرب د A او B مساوی صفردی. مګرA او B صفرنه دي.R تبديلی رينګ نه دی. ځکه:

$$B.A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq A.B$$

مثال: (D,+,.) او (S,+,.) integral domain چې عينيت عناصر يی $0_D \in D$ ، $0_S \in S$ او واحد (unity) عناصريی 1_D ، 1_S دي. پر R:= DxS باندې دا لاندې دوه ګوني رابطي تعريف شوي دي

$$+ : R \times R \longrightarrow R$$
$$(a,b) \longmapsto a+b$$

$$\cdot : R \times R \longrightarrow R$$
$$(a,b) \longmapsto a \cdot b$$

یعني که $a = (d_1, s_1)$ او $b = (d_2, s_2)$ وي.بیا :

$a + b = (d_1,s_1) + (d_2,s_2) = (d_1+d_2, s_1+s_2)$

$a \,.\, b = (d_1,s_1) \,.\, (d_2,s_2) = (d_1.d_2, s_1.s_2)$

(R,+,.) یو تبدیلی رینګ (commutative ring) دی چې عینیت عنصریی $(0_D,0_S)$ او واحد عنصریی $(1_D,1_S)$ دی. مګر integral domain نه دی. ځکه:

$(1_D,0_S) \,.\, (0_D,1_S) = (1_D \,.\, 0_D, 0_S \,.\, 1_S) = (0_D,0_S)$

یعني لیدل کیږي چې $(1_D,0_S)$ او $(0_D,1_S)$ خلاف د صفردي. مګرحاصل ضرب یی مساوی صفردی.

تعریف: $(R,+,.)$ یوintegral domain دی.که یوه $\varphi: R \longrightarrow \mathbb{N}_0$ تابع دلاندي خواصوسره موجوده وي:

$(\,i\,)\ \varphi(a) \leq \varphi(a.b) \qquad (\forall\, a,b \in R \setminus \{0\})$

$(\,ii\,)\ \forall\, a,b \in R \setminus \{0\} \ ,\exists q,r \in R\,;\ a = bq + r$

دلته د $r \neq 0$ لپاره باید $\varphi(r) \leq \varphi(b)$ وي

R د φ سره یوځای د Euclidean Domain په نامه یادیږي. مونږهغه په (R, φ) سره ښیو.

مثال: مونږپوهیږوچې $(\mathbb{Z},+,.)$ یو اینتګرال دومین دی. غواړو ثبوت کړو، چې $\mathbb{Z}$ نظرلاندي تابع ته یو Euclidean Domain دی:

$$\varphi: \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0$$
$$a \longmapsto |a|$$

$0 \neq a,b \in \mathbb{Z}$

$\varphi(a) = |a| \leq |a|.\,|b| = |ab| = \varphi(ab) \Longrightarrow$ (i)

اوس غواړو (ii) ثبوت کړو . د division algorithm له مخې:

$\exists q, r \in \mathbb{Z}\,;\; a = bq + r \quad (\,0 \leq r < b\,)$

$r = 0 \Longrightarrow \varphi(0) = |0| < \;|b| = \varphi(b)$ [ځکه $b \neq 0$]

$r \neq 0 \;\Longrightarrow\; \varphi(r) = |r| < |b| = \varphi(b)$ [ځکه $0 \leq r$]

په نتیجه کې $(\mathbb{Z}, \varphi)$ یو Euclidean Domain دی.

تعریف 6.12 : $(R, +, .)$ یو رینګ چې "1" یی واحد (unity) عنصر دی. **R** معین مشخصات (finite characteristic) لرې، که چیرې یو $n \in \mathbb{N}$ د لاندې خاصیت سره موجود وي.

$0 = 1+1+1+\ldots+1$ (n terms ((دفعه) وار n))

یعني $n.1 = 0$ وي

ترټولوکوچنۍ هغه ډول n ته د R مشخصه (charactiristic) ویل کیږي. یعني :

char(R): = min{$n \in \mathbb{N}$ | n.1=0}

که هغه ډول یو n موجود نه وي. په هغه صورت بیا R غیر معین مشخصه (infinite characteristic) لري اوورته zero characteristic هم واي.

یعني char(R)=0

مثال : د $\mathbb{Z}$ رینګ غیرمعینه مشخصه (infinite characteristic) لرې . ځکه هیڅ $n > 0$ نه پیداکیږي چې $n\,.1=0$ شي .

1 , 1+1 , 1+1+1 , 1+1+1+1, ... = 1,2,3,4, . . .

لیدل کیږي چې هیڅ تکرار صورت نه نسې. پس char($\mathbb{Z}$)= 0

که د $\mathbb{Z}_n$ رینګ په نظرکې ونیسو

$\bar{1} \quad, \bar{1} + \bar{1}\,, \bar{1} + \bar{1} + \bar{1}, \bar{1} + \bar{1} + \bar{1} + \bar{1}, \quad . \;.\; .$

دلته پس د n وارې (دفعه) تکرار صورت نیسي. یعنې:

$\bar{0}\,, \bar{1}, \bar{2}, \bar{3}, .\;.\;.\;.\;., \overline{(n-1)}\,, \bar{0}, \bar{1}, \bar{2}, \bar{3}, .\;.\;.\;.\;.\;, \overline{(n-1)}, \bar{0}$

يعني $\bar{0}$ = ($\bar{1}$. n) . پس $\mathbb{Z}_n$ رينګ finite characteristic (معينه مشخصه) لري . يعني $char(\mathbb{Z}_n) = n$

قضيه 6.7 : (R,+,.) يو رينګ دی چې واحد (unity) عنصر او معينه مشخصه (characteristic) لري. يعنې char (R) = p≠ 0 . بيا:

(a) p . a = 0 $\forall a \in R$

(b) R $\text{integral domain} \Rightarrow p \in P$ [يو لمړنی عدد p]

ثبوت (a)

$a \in R \Rightarrow p.a = p.(1.a) = (p.1).a = 0.a = 0$

ثبوت (b)

$\exists r,s \in \mathbb{N}\,; p = r.s$

$\Rightarrow 0 = p.1 = (r.1).(s.1)$

$\Rightarrow r.1 = 0 \lor s.1 = 0$ [ځکه R يو $integ - dom$ دی]

له هغه څخه نتيجه اخلو چې r اويا s هم د R مشخصه (charact) ده . ځرنګه چې $r.s \leq p$ دی پس بايد r = p اويا s = p وي. په نتيجه کې p يولمړنی (اوليه) عدد دی .

ليما 6.4 : (D,+,.) يو integral Domain دی.بيا :

a,b,c $\in D$, $c \neq 0$ $a.c = b.c$ $\Rightarrow a = b$

يعنې integral domain نظر "." ته اختصار پذير دی .

ثبوت :

a.c = b.c ⇒ a.c - b.c = 0

0 = a.c - b.c = (a - b) .c

$\Rightarrow a - b = 0 \lor c = 0$ [ځکه D يو integral domain]

$\Rightarrow a - b = 0$ [ځکه c≠ 0]

$\Rightarrow a = b$

نوټ: 6.4 ليما د رينګ لپاره صدق نه کوی. يعنې رينګ اختصارپذيرنه دی. دمثال په ډول په (. ,+, $\mathbb{Z}_6$) رينګ کې:

$\bar{2}\,.\,\bar{3} = \bar{6} = \bar{0} = \overline{12} = \bar{3}\,.\,\bar{4}$

مګر $\bar{2} \neq \bar{4}$ دی

ليما 6.5 : (R,+,.) يو رينګ د unity (واحد) سره , I په R کې يو اديال او $I \neq \{0\}$. که I يو معکوس پذير (invertible) عنصر ولري. په هغه صورت بيا I=R دی. يعنې :

$\exists a \in I \land b \in R; a.b = 1 \Rightarrow I = R$

ثبوت :

$a \in I \ \wedge \ a\ invertible \ \Rightarrow \ \exists b \in R; ba = 1$
$x \in R \Rightarrow x = x.1 = x.(b.a)$
$= (xb).a \in I$ [ځکه I یو ایدیال دی]
$\Rightarrow R \subseteq I$

له بلې خوا پوهیږو چې $I \subseteq R$ دی. پس R = I

مثال: (D,+,.) یو integ-dom دی. $a,b \in D$
(a) که $char(D)$ غیرمعین وی. دمثال په ډول ℝ حقیقي اعداد . بیا د Binomial فورمول په اساس:

$(a+b)^2 = a^2 + 2.ab + b^2$
$(a+b)^3 = a^3 + 3.a^2b + 3ab^2 + b^3$

(b) که $char(D) = 2$ وې. بیا:

$(a+b)^2 = a^2 + 2.ab + b^2 = a^2 + 0 + b^2 = a^2 + b^2$
ځکه $char(D) = 2$ دی. پس د 6.7 قضی له مخی باید $2ab = 0$ وې
(c) که $char(D) = 3$ وې. بیا:

$(a+b)^3 = a^3 + 3.a^2b + 3ab^2 + b^3$
$= a^3 + 0 + 0 + b^3 = a^3 + b^3$
ځکه $char(D) = 3$ دی. پس د 6.7 قضی له مخی باید $3.a^2b = 0$
او $3ab^2 = 0$ وې

لیدل کیږي چې په الجبر کې د Binomial فورمول تابع د integral domain (اویا Field) د مشخصه (characteristic) دی. اوس غواړودا حالت په عمومي ډول مطالعه کړو.

لیما 6.6: (D,+,.) یو integ-dom او $char(R) = p \neq 0$ دی. بیا :

(a) $(a+b)^p = a^p + b^p$ $(\forall a,b \in D)$
(b) $\varphi: D \to D$
$x \to x^p$

φ یو $D - monom$ (یعني $D - Hom$ او $injective$) دی. φ د *frobenius function* په نوم یادیږي .

ثبوت (a) : ځرنګه چې D تبدیلی دی. پس:

$\forall a,b \in D \ , (a.b)^p = b^p.a^p = a^p.b^p$

د *binomial formel* له مخې ليکی شو:

$$(a+b)^p = a^p + pa^{p-1}.b + \frac{p.(p-1)}{2!}\, a^{p-2}.b^2 + \frac{p.(p-1).(p-2)}{3!}\, a^{p-3}.b^3 + \cdots + pab^{p-1} + b^p$$

که په پورتني معادله کې د a^p او b^p څخه صرف نظروشي. بيا نور هريو په عمومي ډول لاندي شکل لري:

$$\frac{p.(p-1).(p-2).....(p-r+1)}{1.2.3....r}\, a^{p-r}.b^r$$

البته دلته $1 \leq r \leq p-1$ فرض شوی دی

$$k := \frac{(p-1).(p-2).....(p-r+1)}{1.2.3....r} \qquad , s := 1.2.3....r$$

د *binomial formel* په اساس p.k يومثبت تام عدد دی. پس بايد p.k پر s قابل د تقسيم وې. څرنګه چې $p>r$ او د 6.7 قضی له مخې يو اوليه عدد دی. پس بايد k پر s باندې قابل د تقسيم وې. يعني:

$k = \frac{(p-1).(p-2).....(p-r+1)}{1.2.3....r}$ يوطبعې عدد دی. پس د 6.7 قضيی له مخې:

$$\frac{p.k}{s}\, a^{p-r}.b^r = \frac{p.(p-1).(p-2).....(p-r+1)}{1.2.3....r}\, a^{p-r}.b^r = 0$$

$$(a+b)^p = a^p + 0 + 0 + \cdots + 0 + b^p = a^p + b^p$$

ثبوت (b) :

$$x, y \in D\,;\ \varphi(x+y) = (x+y)^p = x^p + y^p \quad [\ \text{د}\ (a)\ ]$$

$$= \varphi(x) + \varphi(y)$$

$$\varphi(x.y) = (x.y)^p = y^p.\ x^p = x^p.y^p \quad [\ \text{ځکه}\ D\ \text{تبديلی}\ ]$$

$\Longrightarrow \varphi$ R-Hom

$: \varphi \ injective$

$x \in ker\varphi \Rightarrow \ \varphi(x) = 0 \ \wedge \ \varphi(x) = x^p$

$\Rightarrow 0 = x^P = x.x.x \dots . x$ [دفعه p]

$\Rightarrow x = 0$ [$integ - dom$ يو D]

$\Rightarrow \ker\varphi = \{0\}$

له دي څخه د 2.3 قضيې له مخې نتيجه اخلوچې φ يو injective دی .
په نتيجه کې φ يو R-monom دی

مثال : غواړو $(\bar{2})^9$ په $\mathbb{Z}_3$ کې پيدا کړو. څرنګه چې $\mathbb{Z}_3$ يو Integ-Domain او **3** = Char($\mathbb{Z}_3$) دی . پس کولای شو د حل لپاره 6.6 ليما څخه استفاده وکړو

$(\bar{2})^9 = ((\bar{2})^3)^3 = ((\bar{1} + \bar{1})^3)^3$

$= ((\bar{1})^3 + (\bar{1})^3)^3 = (\bar{1})^3 + (\bar{1})^3 = \bar{2}$

تمرين 6.9: د حل لپاره د 6.6 ليما څخه استفاده وکړی

(a) $(\bar{2})^{49}$ په $(\mathbb{Z}_7,+,.)$ کې پيدا کړی

(b) $(\bar{2})^8$ په $(\mathbb{Z}_2,+,.)$ کې پيدا کړی

(c) $(\bar{3})^{25}$ په $(\mathbb{Z}_5,+,.)$ کې پيدا کړی

(d) (D,+,.) يو integ-dom او $char(D) = 11$ ده. a,b∈D
$(a+b)^{121}$ پيدا کړی

مثال: اوس غواړودا لاندې خطی معادلات په $\mathbb{Z}_5$ کې حل کړو

$x + \bar{3}y = \bar{2}$
$\bar{3}x + \bar{2}y = \bar{2}$

$\bar{3}X + \bar{3}.\bar{3}y = \bar{3}.\bar{2} = \bar{6} = \bar{1}$
$\bar{3}X + \bar{2}y = \bar{2}$

$\bar{3}x + \bar{4}.y = \bar{1}$
$\bar{3}x + \bar{2}y = \bar{2}$

$\bar{3}x + \bar{4}.y = \bar{1}$
$-\bar{3}x - \bar{2}y = -\bar{2}$

$\bar{2}\,y = -\,\bar{1} = \bar{4} \quad \Rightarrow \quad \bar{3}.\bar{2}\,y = \bar{3}.\bar{4} \quad \Rightarrow y = \bar{2}$

$\bar{3}x + \bar{2}.\bar{2} = \bar{2}$

$\Rightarrow \bar{3}x = \bar{2} - \bar{4} = -\,\bar{2} = \bar{3} \quad [\bar{2} + \bar{3} = \bar{0} \Rightarrow -\,\bar{2} = \bar{3}$ ځکه]

$\Rightarrow \bar{2}.\bar{3}x = \bar{2}.\bar{3} \Rightarrow x = \bar{1}$

مثال:

$\bar{3}x + \bar{2}.y = \bar{0}$

$\bar{2}x + \bar{1}y = \bar{4}$

لمړی غواړوپورتنی معادلي د $(\mathbb{Z}_7, +, .)$ په رینګ کی حل کړو. اول لمړی معادله په $\bar{2}$ کی ضربو اودویمه معادله په $\bar{3}$ ضربو

$\bar{6}x + \bar{4}.y = \bar{0}$

$\bar{6}x + \bar{3}y = \bar{4}.\bar{3} = \overline{12} = \bar{5}$

$\bar{6}x + \bar{4}.y = \bar{0}$

$-\bar{6}x - \bar{3}y = \bar{4}.\bar{3} = \overline{12} = -\bar{5}$

$y = -\,\bar{5} = \bar{2} \qquad [\bar{5} + \bar{2} = \bar{0} \Rightarrow \bar{2} = \bar{2} - \bar{5}$ ځکه]

$\bar{3}x + \bar{2}.y = \bar{0}$

$\Rightarrow \bar{3}x = -\,\bar{2}.y = -\,\bar{2}.\bar{2}. = -\bar{4}. = \bar{3}$

$\bar{5}.\bar{3}.x = \bar{5}.\bar{3} \Rightarrow x = \bar{1}$

اوس غواړوپورتنی معادلي د $(\mathbb{Z}_5, +, .)$ په رینګ کی حل کړو . لمړی معادله د $\bar{2}$ اودویمه معادله $\bar{3}$ سره ضربو

$\bar{6}x + \bar{4}.y = \bar{0} \qquad \Rightarrow \bar{1}x + \bar{4}.y = \bar{0}$

$\bar{6}x + \bar{3}y = \bar{4}.\bar{3} = \overline{12} \quad \Rightarrow \bar{1}x + \bar{3}y = \bar{2}$

$\bar{1}x + \bar{4}.y = \bar{0}$

$-\bar{1}x - \bar{3}y = -\,\bar{2}$

$\Rightarrow y = -\,\bar{2} = \bar{3} \wedge x = -\,\bar{4}.y = -(\bar{4}.\bar{3}) = -\,\bar{2} = \bar{3}$

نوټ:

(a) څرنګه چې د $(\mathbb{Z}_6, +, .)$ رینګ یو integ-Domain نه دی ، پس:

$\bar{4}x = \bar{0} \Rightarrow x = \bar{0} \vee x = \bar{3}$

(b) ځرنګه چې د $(\mathbb{Z}_5, +, .)$ رینګ یو integ-Domain دی ، پس:

$\bar{4}x = \bar{0} \Rightarrow x = \bar{0}$

مثال: دالاندي خطی معادلي په $(\mathbb{Z}_7, +, .)$ کی د متریکس له لیاری حل کوو

$$\begin{aligned} x - \bar{2}y + \bar{2}z &= \bar{3} \\ \bar{3}x - y + \bar{2}z &= \bar{4} \\ \bar{2}x + y - z &= \bar{1} \end{aligned}$$

د ضرایبو متریکس یي لاندي شکل لري

$$A = \begin{pmatrix} \bar{1} & -\bar{2} & \bar{2} \\ \bar{3} & \bar{1} & \bar{2} \\ \bar{2} & \bar{1} & -\bar{1} \end{pmatrix}, \quad b = \begin{pmatrix} \bar{3} \\ \bar{4} \\ \bar{1} \end{pmatrix}$$

$$(A, b) = \begin{pmatrix} \bar{1} & -\bar{2} & \bar{2} & \bar{3} \\ \bar{3} & \bar{1} & \bar{2} & \bar{4} \\ \bar{2} & \bar{1} & -\bar{1} & \bar{1} \end{pmatrix}$$

اول لمړی کرښه په $\bar{3}$ - کی ضربواود دویمی کرښی سره جمع کوو . بیا لمړی کرښه په منفی $\bar{2}$ - کی ضربواود دریمی کرښی سره جمع کوو

$$\begin{pmatrix} \bar{1} & -\bar{2} & \bar{2} & \bar{3} \\ \bar{0} & \bar{0} & -\bar{4} & -\bar{5} \\ \bar{0} & \bar{5} & -\bar{5} & -\bar{5} \end{pmatrix}$$

$-\bar{4}z = \bar{3}z = -\bar{5} = \bar{2} \Longrightarrow \bar{3}.(\bar{3})^{-1}.z = \bar{2}.(\bar{3})^{-1}$

$\Longrightarrow z = \bar{2}.\bar{5} \quad [\bar{3}.\bar{5} = \bar{1} \Rightarrow (\bar{3})^{-1} = \bar{5}$ ځکه $]$

$\Longrightarrow z = \overline{10} = \bar{3}$

$\bar{5}y = \bar{5}z - \bar{5}$

پورتنی معادله په $(\bar{5})^{-1}$ کی ضربو

$\bar{5}.(\bar{5})^{-1}y = \bar{5}.(\bar{5})^{-1}z - \bar{5}.(\bar{5})^{-1}$

$\Longrightarrow y = z - \bar{1} = \bar{3} - \bar{1} = \bar{2}$

$x = \bar{3} + \bar{2}y - \bar{2}z = \bar{3} + \bar{4} - \bar{2}.\bar{3} = \bar{7} - \bar{6} = \bar{1}$

تمرین 6.10:

(a) دا لاندي معادلي په $(\mathbb{Z}_7,+,.)$ کی حل کړی

$\overline{3}\,x+\overline{6}y = \overline{6}$
$\overline{4}x+\overline{5}y = \overline{4}$

(b) دا لاندي معادلي په$(\mathbb{Z}_5,+,.)$ کی حل کړی

$\overline{3}\,x+\overline{1}y = \overline{2}$
$\overline{2}x-\overline{3}y = \overline{1}$

(c) دا لاندي خطی معادلي ذیل په $(\mathbb{Z}_7,+,.)$ کی د متریکس له لیاری حل کړی

$$\overline{2}x+y+\overline{3}\,z=\overline{5}$$
$$x-y+z=\overline{4}$$
$$x+\overline{3}y+z=\overline{5}$$

تعریف 6.13 : (R,+,.) یو رینګ چې واحد (unity) "1" لري.

$$\text{R[x]}:=\{\,P(x)=\sum_{i\in\mathbb{N}_0}a_i\,x^i\;\big|\;a_i\in R\,\}$$

R[x] نظر "+" او "." یو تبدیلی رینګ (Commutative Ring) دی چې واحد (unity)عنصریی P(x) = 1 دی

(R[x],+,.) ته Polynomial Ring ویل کیږي
$p(x)\in$ R[x] د Polynomial (پولینوم) نظر R رینګ ته یادیږي .

مثال: ($\mathbb{Z}$ [x],+,.) یو Polynomial Ring نظر $\mathbb{Z}$ (تام اعداد) ,
($\mathbb{Q}$ [x],+,.) نظر $\mathbb{Q}$ (ناطق اعداد) , ($\mathbb{R}$ [x],+,.) نظر $\mathbb{R}$ (حقیقی اعداد)
او ($\mathbb{Z}_7$ [x],+,.) نظر $\mathbb{Z}_7$ ته دی. دمثال په ډول:

$f_1(x)=5+2x+3x^2\in\mathbb{Z}[x]$

$f_2(y)=2+\frac{1}{2}y+y^3\in\mathbb{Q}[y]$

$f_3(z)=2+\sqrt{2}\,\frac{1}{2}z^2+\sqrt{3}z^5\in\mathbb{R}\,[z]$

$f_4(t)=\overline{3}+\overline{2}\,t^2+\overline{4}t^3\in\mathbb{Z}_7[\mathbf{t}]$

تعریف 6.14 : (R,+,.) یو رینګ چې واحد (unity)عنصر یی "1" او (R[x],+,.) د هغه Polynomial Ring دی

$$P(x) = \sum_{i\in\mathbb{N}_0} a_i\, x^i \in \mathrm{R[x]}$$

درجه (degree) د $P(x)$ په لاندي ډول تعریف شوی ده:
که $P(x) \neq 0$ وي

deg (p(x)) = max{ $i \in \mathbb{N}_0 \mid a_i \neq 0$ }

که $P(x) = 0$ وي. بیا deg (p(x)) = - ∞ تعریف شوې ده
پولینوم چې درجه یی صفروی د Constant Polynomail (ثابت پولینوم)
په نوم یادیږي. د مثال په ډول p(x) = c (c∈ R)
که مونږ دوه پولینومه Q(x) , P(x) ∈ R[x] ولرو چې درجه د P(x) مساوی m او د Q(x) مساوی n وي. بیا :

deg(P(x).Q(x)) ≤ m + n ∧ deg(P(x) + Q(x)) ≤ max(m,n)

مثال : د ($\mathbb{Z}_6$ [x],+,.) په رینګ دوه لاندي پولینومی راکړل شوي دي

$P(x) = \bar{2}\,x^2 + \bar{1}$, $q(x) = \bar{3}\,x + \bar{1}$

deg(p(x)) = 2 , deg(q(x)) = 1

$$\begin{aligned} P(x).q(x) &= \bar{2}\,x^2 . \bar{3}\,x + \bar{1}.\bar{3}\,x + \bar{1} . \bar{2}\,x^2 + \bar{1}.\bar{1} \\ &= \bar{6}. X^3 + \bar{2}\,x^2 + \bar{3}\,x + \bar{1} \\ &= \bar{2}\,x^2 + \bar{3}\,x + \bar{1} \end{aligned}$$

لیدل کیږي چې deg(p(x).q(x)) < deg(p(x)) + deg (q(x))

قضیه 6.8 :

integ-Domain (D,+,.) ⇒ (D[x],+,.) integ-Domain

ثبوت : مونږ پوهیږو چې D[x] یو تبدیلی رینګ د واحد عنصرسره دی. اوس ثبوت کو:

$$g(x), f(x) \in D[x] , f(x) \neq 0 \wedge g(x) \neq 0 \Rightarrow f(x) . g(x) \neq 0$$

$$f(x) := a_0 + a_1x + a_2x^2 + - - - - - + a_{m-1}x^{m-1}$$

$+ a_m x^m \quad (a_m \neq 0)$

$g(x) := b_0 + b_1x + b_2x^2 + - - - - - + b_{n-1}x^{n-1}$

$+ b_n x^n \quad (b_n \neq 0)$

$a_m \neq 0 \;\; \wedge \;\; b_n \neq 0$

$\Rightarrow a_m . b_n \neq 0$ [ځکه D یو integ-domain دی]

$a_m . b_n \neq 0 \quad \Rightarrow a_m . b_n . x^{m+n} \neq 0$

$\Rightarrow f(x) . g(x) \neq 0$

$\Rightarrow$ D[x] is integ-Domain

نوټ: $Q(x) , P(x) \in D[x]$.

$deg(P(x).Q(x)) = deg(P(x)) + deg(Q(x))$

ځکه:

$a_m \neq 0 \;\; \wedge \;\; b_n \neq 0$

$\Rightarrow a_m . b_n \neq 0 \Rightarrow a_m . b_n . x^{m+n} \neq 0$

$\Rightarrow deg(P(x).Q(x)) = m + n = deg(P(x)) + deg(Q(x))$

$deg(P(x).Q(x)) = deg(P(x)) + deg(Q(x))$

مثال: غواړو حل د لاندي پولینوم په $\mathbb{Z}_7$ کې پیداکړو

$P(x) \in \mathbb{Z}_7 \; [x]$

$P(x) = x^2 + x + \bar{2} \quad = (x - \bar{3})^2$

ځکه:

$(x - \bar{3})^2 = x^2 - \bar{2}. \bar{3}x + \bar{3}. \bar{3}$

$= x^2 - \bar{6}x + \bar{9}$

$= x^2 - \bar{6}x + \bar{2}$

$= x^2 + \bar{1}x + \bar{2}$

پس حل يی:

$x^2 + x + \bar{2} = (x - \bar{3})^2 = \bar{0} \quad \Rightarrow \; x = \bar{3}$

نوټ : غواړم $\bar{1} = \bar{6}$ - تشریح کړم

$\bar{6} + \bar{1} = \bar{0} \;\; \Rightarrow \; \bar{1} = \bar{0} - \bar{6} = - \bar{6}$

دحل امتحان :

$x^2 + x + \bar{2} = \bar{3}.\bar{3} + \bar{3} + \bar{2} = \bar{9} + \bar{3} + \bar{2}$
$= \bar{2} + \bar{3} + \bar{2} = \bar{7} = \bar{0}$

که $P(x) = x^2 + x + 2 \in \mathbb{R}[x]$ وي.

$$x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a} = \frac{-1 \pm \sqrt{1^2-4.1.2}}{2.1} = \frac{-1 \pm \sqrt{-7}}{2}$$

لیدل کیږي چې P(x) په حقیقی اعدادو کې حل نه لري

مثال :

(a) غواړود $P(x) = x^2 - \bar{1} \in \mathbb{Z}_8[x]$ پولینوم حل په ($\mathbb{Z}_8$,+,.) رینګ کی پیدا کړو .

$x^2 - \bar{1} = \bar{0} \Longrightarrow x^2 = \bar{1}$

$(\bar{1})^2 = \bar{1}, (\bar{3})^2 = \bar{9} = \bar{1}, (\bar{5})^2 = \overline{25} = \bar{1}, (\bar{7})^2 = \overline{49} = \bar{1}$

لیدل کیږي چې P(x) په $\mathbb{Z}_8$ رینګ کی څلور حله لری

(b) اوس غواړود $P(x) = x^2 - \bar{1} \in \mathbb{Z}_7[x]$ پولینوم حل په ($\mathbb{Z}_7$,+,.) انتګرال دومین کی پیداکړو

$x^2 - \bar{1} = \bar{0} \Longrightarrow x^2 = \bar{1}$

$(\bar{1})^2 = \bar{1}, (\bar{6})^2 = \overline{36} = \bar{1}$

P(x) په $\mathbb{Z}_7$ رینګ کی فقط دوه حله لري

نوټ: په عمومی صورت کولای شو ووایو چې دیوی n درجه یی پولینوم حل شمیر د n څخه کوچنی اویا د n سره مساوی دی

تمرین 6.11:

(a) د لاندي پولینوم حل په $\mathbb{Z}_7$ رینګ کی پیدا کړی .

$P(x) \in \mathbb{Z}_7[x]$, $P(x) = x^2 + \bar{2}x + \bar{4}$

(b)

$Q(x), P(x) \in \mathbb{Z}_6[x]$
$P(x) = \bar{2}x^2 + \bar{1}$, $Q(x) = \bar{3}x^2 + \bar{1}$

P(x).Q(x) را دریافت نماید

قضیه 6.9 (Division Algorithm) **:** (D[x],+,.) یو integ-Domain دی. بیا :

$a(x),b(x) \in D[x]$, $b(x) \neq 0$

$\Rightarrow \exists\ q(x),r(x) \in D[x]\ ;\ a(x) = b(x).q(x) + r(x)$

دلته $r(x) = 0$ اویا $deg(r(x)) < deg(b(x))$ ده

مونږ دالاندي پولینومونه په نظرکی نیسو :

$$a(x) := a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m \quad (a_m \neq 0\,)$$

$$b(x) := b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1} + b_n x^n \quad (b_n \neq 0\,)$$

غواړو دا قضیه د complete induction له لیاری نظر پولینوم درجه ته ثبوت کړو.

په complete induction ثبوت کی دا دري لاندي حالتونه موجود دي
لمړی : باید **د** $deg(a(x)) = 0$ لپاره صدق وکړی
دویم : مونږ فرض کوو دټولو پولینومو لپاره چي درجه یی $m - 1$ وی ، صدق کوی
دریم : باید ثبوت شی چي د $a(x)$ لپاره هم صدق کوی
لمړی حالت:

$$deg(a(x)) = 0 \Rightarrow a(x) = a_0$$

پدی حالت کی د $b(x)$ لپاره دوه لاندي امکانات موجود دي:

(a) $deg(a(x)) = deg(b(x)$

$$\Rightarrow b(x) = b_0 \Rightarrow a(x) = q.b(x)\ ,\ q = \frac{a_0}{b_0}$$

دلته $b_0 \neq 0$ دی. ځکه $b(x) \neq 0$ فرض شویده

(b) $deg(a(x)) < deg(b(x))$

$$\Rightarrow a(x) = 0.b(x) + r(x)\ ,\ q(x) = 0,\ r(x) = a(x)$$

پس لمړی حالت صدق کوي. اوس فرض کوو دټولو پولینومو لپاره چي درجه یی $m - 1$ وی ، صدق کوي
اوس غواړو ثبوت کړو چي د $deg(a(x)) = m$ لپاره هم صدق کوی. پورته مو د $deg(a(x)) = 0$ حالت ثبوت کړ . اوس د $deg(a(x)) > 0$ حالت په نظر کي

نیسو . پورته مو ولیدل چې قضیه د $deg(a(x)) < deg(b(x))$ لپاره صدق کوی. اوس باید د $deg(b(x)) < deg(a(x))$ حالت ثبوت کړو. مونږ دالاندي تابع په نظرکی نیسو:

$$f(x) = a(x) - \frac{a_m}{b_n} x^{m-n} . b(x)$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m$$

$$- \frac{a_m}{b_n} (b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1} + b_n x^n). x^{m-n}$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m$$

$$- \frac{a_m}{b_n} (b_0 + b_1x \ + - - - + b_{n-1}x^{n-1}) - \frac{a_m}{b_n} b_n x^n). \ x^{m-n}$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m$$

$$- \frac{a_m}{b_n} (b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1}) - a_m x^m$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1}$$

$$- \frac{a_m}{b_n} (b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1})$$

$\Longrightarrow \ deg(f(x)) = m -1$

$\Longrightarrow \exists \ p(x),r(x) \in \ D[x] ;$

$f(x) = b(x).p(x) + r(x)$ [د فرضی حالت له مخی]

دلته $r(x) = 0$ اویا $deg(r(x)) < deg(b(x))$ ده

$$b(x).p(x) + r(x) = f(x) = a(x) - \frac{a_m}{b_n} x^{m-n} . b(x)$$

$$\Longrightarrow a(x) = b(x).p(x) + r(x) + \frac{a_m}{b_n} x^{m-n} . b(x)$$

$$= b(x)\left(p(x) + \frac{a_m}{b_n} x^{m-n} \right) + r(x)$$

که مونږ $q(x) = p(x) + \frac{a_m}{b_n} x^{m-n}$ وضع کړو. بیا

$$a(x) = b(x).q(x) + r(x)$$

مثال:

$a(x) = \ x^3 + 4x^2 + 5x + 7 \ , b(x) = x + 1 \in \mathbb{Z}[x]$

$x^3 + 4x^2 + 5x + 7 : x + 1 = x^2 + 3x + 2$ $-(x^3 + x^2)$

$3x^2 + 5x$
$-(3x^2 + 3x)$

$2x + 7$
$-(2x + 2)$

5

دلته $q(x) = x^2 + 3x + 2$ او $r(x) = 5$ لاس ته راځی. یعنې:

$a(x) = q(x).b(x) + r(x)$

قضیه 6.10 (the Remainder Theorem):

(D[x],+,.) یو integ-Domain ، $f(x) \in D[x]$ او $c \in D$. بیا :

(1) $\exists\, q(x) \in D[x]\ ;\ f(x) = (x-c) . q(x) + f(c)$

(2) $(x-c) | f(x) \iff f(c) = 0$

ثبوت (1) :

$\exists\, q(x), r(x) \in D[x]\ ;$

$f(x) = (x-c) . q(x) + r(x)$ [د Division Algorithm قضیی له مخی]

د r(x) لپاره دوه لاندې حالتونه امکان لري :

$r(x) = 0 \implies f(c) = (c - c) . q(x) + 0 = 0$

$r(x) \neq 0 \implies \deg(r(x)) < \deg(x - c) = 1 \implies \deg(r(x)) = 0$
$\implies r(x) = r_0$

$f(c) = (c - c) . q(x) + r_0 = r_0$

$f(x) = (x-c) . q(x) + r(x) = (x-c) . q(x) + r_0$

$= (x-c) . q(x) + f(c)$

ثبوت (2) :

" ⟹„ د **(1)** له مخی لیکلی شو :

$\exists\, q(x) \in D[x]\, ;\, f(x) = (x-c) . q(x) + f(c)$

څرنګه چې f(x) پر (x-c) باندی قابل دتقسیم دی. پس باید f(c) = 0 وی

" ⟸„

$f(x) = (x-c) . q(x) + f(c)$ [د (1) له مخی]

$= (x-c) . q(x) + 0$

$\Longrightarrow (x - c) \mid f(x)$

مثال:

$f(x) = 2x^5 + x^4 + 7 x^3 + 2x + 10$

$f(-1) = 2(-1)^5 + (-1)^4 + 7(-1)^3 + 2.(-1) + 10 = -2 + 1 - 7 -2 + 10 = 0$

$\Longrightarrow x + 1 \mid f(x)$

تعریف 6.15 : (D[x],+,.) یو integ-Domain

$f(x),g(x) \in D[x],\ g(x) \neq 0$,

(a) f(x) پر g(x) د تقسیم وړده، په دی شرط چې یوه تابع h(x) ∈ D[x] د لاندي خواصو سره موجوده وی:

$f(x) = h(x).g(x)$

(b) d(x) ∈ D[x] د (x) او g(x) د common divisor (مشترک قاسم) په یادیږی ، پدی شرط چې f(x) او g(x) پر d(x) تقسیم وړ وی. یعنې:

$d(x) \mid f(x) \ \wedge\ d(x) \mid g(x)$

(c) d(x) د greatest common divisor (gcd) (ترټولو لوی مشترک قاسم) په نامه یادوې ، په دې شرط چې لاندي افاده صدق وکړی:

$h(x) \in D[x]\ ,\ h(x) \mid f(x)\ \wedge\ h(x) \mid g(x) \Longrightarrow h(x) \mid d(x$

مثال:

$p_1(x) = 2x^3 +10x^2 + 2x +10\ ,\ p_2(x) = x^3 - 2x^2 + x - 2 \in \mathbb{Q}\,[x]$

غواړو f(x),g(x) ∈ ℚ [x] پیدا کړو چې :

$gcd(p_1(x), p_2(x)) = f(x).\, p_1(x) + g(x).\, p_2(x)$

$2x^3 + 10x^2 + 2x + 10 = 2(x^3 - 2x^2 + x - 2) + (14x^2 + 14)$

$x^3 - 2x^2 + x - 2 = (\frac{1}{14}x - \frac{1}{7}).(14x^2 + 14)$

$\Longrightarrow \gcd(p_1(x), p_2(x)) = 14x^2 + 14$

$14x^2 + 14 = 1.(2x^3 + 10x^2 + 2x + 10) - 2(x^3 - 2x^2 + x - 2)$

$\Longrightarrow$ **f(x) = 1 , g(x) = -2**

$\Longrightarrow \gcd(p_1(x), p_2(x)) = 14x^2 + 14 = f(x).\, p_1(x) + g(x).\, p_2(x)$

مثال:

$p_1(x) = x^4 + x^3 + x + 1 \,,\, p_2(x) = x^2 + x + 1 \in \mathbb{Q}[x]$

غواړو $f(x), g(x) \in \mathbb{Q}[x]$ پیدا کړو چې :

$\gcd(p_1(x), p_2(x)) = f(x).\, p_1(x) + g(x).\, p_2(x)$

$x^4 + x^3 + x + 1 = (x^2 - 1).(x^2 + x + 1) + (2x + 2)$

$x^2 + x + 1 = \frac{x}{2}.(2x + 2) + 1$

$(2x + 2) = (2x + 2).1$

$\Longrightarrow \gcd(p_1(x), p_2(x)) = 1$

$$1 = (x^2 + x + 1) - \frac{1}{2}x.(2x + 2)$$
$$= (x^2 + x + 1) - \frac{1}{2}x((x^4 + x^3 + x + 1) - (x^2 - 1).(x^2 + x + 1))$$
$$= (x^2 + x + 1) + (\frac{1}{2}x^3 - \frac{1}{2}x).(x^2 + x + 1)$$
$$- \frac{1}{2}x(x^4 + x^3 + x + 1)$$
$$= (\frac{1}{2}x^3 - \frac{1}{2}x + 1).(x^2 + x + 1) - \frac{1}{2}x(x^4 + x^3 + x + 1)$$

$\Longrightarrow g(x) = \frac{1}{2}x^3 - \frac{1}{2}x + 1 \,,\, f(x) = -\frac{1}{2}x$

$\gcd(p_1(x), p_2(x)) = 1 = f(x).\, p_1(x) + g(x).\, p_2(x)$

تمرين 6.12

$p_1(x) = x^3 + 5x^2 + 7x + 2$, $p_2(x) = x^3 + 2x^2 + -2x - 1 \in \mathbb{Q}[x]$

$f(x), g(x) \in \mathbb{Q}[x]$ پیدا کڕی چ‌ی :

$\gcd(p_1(x), p_1(x)) = f(x).\, p_1(x) + g(x).\, p_2(x)$

فصل هفتم
ساحه (Field)

تعریف 7.1 : که (.,+,F) یوه تبدیلی حلقه *(commutative Ring)* چې لاندي خواص ولرې د *Field* (ساحه) په نوم یادیږي .

(i) (.,+,F) واحد (unity) عنصر ولرې .

(ii) هر $a \in F-\{0\}$ معکوس پذیر(*Invertible*) ویې . یعنې :

$$\forall\ a \in F-\{0\}, \exists\ b \in F; a.b = 1$$

مثال : (. ,+,Q) , (., + , $\mathbb{R}$) او (., + , $\mathbb{C}$) ساحي (fields) دي . مګر $(\mathbb{Z},+,.)$ ساحه کیداې نشي . ځکه مثال په ډول د $2 \in \mathbb{Z}$ لپاره نظر ضرب "." ته په $\mathbb{Z}$ کې معکوس نشته .

مثال : $(\mathbb{Z}_5,+,.)$ یوه ساحه ده . مګر $(\mathbb{Z}_6,+,.)$ ساحه (Field) نده ځکه د $\overline{2} \in \mathbb{Z}_6$ لپاره په $\mathbb{Z}_6$ کې نظر ضرب ته معکوس موجود نه دی .

تمرین 7.1:

M:= $\{A \in M(2x2,\mathbb{R}) \,|\, A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a^2 + b^2 \neq 0\}$

ثبوت کړئ چې ولی (.,+,M) د متریکسو جمع "+" او ضرب "." له مخی یوه ساحه (Field) نه ده.

تعریف 7.2: (. ,+, F) یوه ساحه (field) ده ، چې "0" د هغه عینیت عنصر نظر "+" او "1" یې واحد عنصرنظر "." دی . $\emptyset \neq H \subseteq F$.

H د subfield (ساحه فرعی) په نوم یادیږي که چیري (. , + , H) په خپله یو ساحه وي. اویا H یوه Subfield د F ده په دې شرط چې :

(1)

(i) $\forall\ a,b \in H \Rightarrow a+b \in H$

(ii) $\forall a \in H \Rightarrow -a \in H$

(2)

(i) $\forall\ a,b \in H \Rightarrow a+b \in H$

(ii) $1 \in H$

(iii) $\forall a \in H \quad a \neq 0 \quad \Rightarrow a^{-1} \in H$

مثال 7.1:

(a) $H \coloneqq \{a + b\sqrt{2} \mid a, b \in Q\}$ یو subfield په $(\mathbb{R}, +, .)$ کې دی.

حل :

$$x, y \in H \Rightarrow \exists\, a, b, c, d \in Q : x = a + b\sqrt{2}\,, y = c + d\sqrt{2}$$

$$x + y = \left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = (a + c) + (b + d)\sqrt{2}$$

$$\Rightarrow\ x + y\ \in H \quad [\ a + b\,, c + d \in Q \quad \text{ځکه}\ ]$$

$\Rightarrow$ (1) (i)

$$x = a + b\sqrt{2}\ \Rightarrow -x = -a + (-b)\sqrt{2} \Rightarrow -x \in H \Rightarrow (1)(ii)$$

$$x.y = \left(a + b\sqrt{2}\right).\left(c + d\sqrt{2}\right) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

$$ac + 2bd\,, ad + bc \in Q\ \Rightarrow x.y\ \in H\ \Rightarrow (2)(i)$$

$$0 \neq x \in H\ \Rightarrow\ \exists a, b \in Q\,; x = a + b\sqrt{2} \neq 0$$

$$\Rightarrow a - b\sqrt{2} \neq 0$$

ځکه غیرله هغه که $a - b\sqrt{2} = 0$ وې . په دې صورت $a = b = 0$ کیږي مګردا د $a + b\sqrt{2} \neq 0$ سره په تضاد کې واقع کیږي.

$$\left(a + b\sqrt{2}\right)^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)}$$

$$= \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2}$$

$$\frac{a}{a^2 - 2b^2}, \frac{(-b)}{a^2 - 2b^2} \in Q\ \Rightarrow\ \left(a + b\sqrt{2}\right)^{-1} \in H\ \Rightarrow \text{(2)(iii)}$$

$$1 = \left(1 + 0.\sqrt{2}\right) \in H \Rightarrow (2)(ii)$$

په نتیجه کی H یوه فرعی ساحه (subfield) ده

(b) د $H \coloneqq \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$ سیت یو integral domain دی، مګر subfield (فرعی ساحه) د $(\mathbb{R}, +, .)$ نه دی .

حل :

په اسانی سره ثبوت کیدای شی چې H یو تبدیلی فرعی رینګ په $\mathbb{R}$ کی دی اوواحد عنصرهم لري. ځکه:

$$1 = \left(1 + 0.\sqrt{2}\right) \in H$$

پس انتګرال دومین هم دی. مګرد (iii)(2) خاصیت صدق نه کوی. ځکه:

$$0 \neq x \in H \;\Rightarrow\; \exists a, b \in \mathbb{Z}\,; x = a + b\sqrt{2} \neq 0$$

$$\Rightarrow a - b\sqrt{2} \neq 0$$

ځکه که $a - b\sqrt{2} = 0$ وی ، په دی صورت باید $a = b = 0$ وی . مګر دا د $a + b\sqrt{2} \neq 0$ سره په تضاد کی واقع کیږی .

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

$$= \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2}$$

$$\frac{a}{a^2-2b^2}, \frac{(-b)}{a^2-2b^2} \notin \mathbb{Z} \;\Rightarrow\; \left(a + b\sqrt{2}\right)^{-1} \notin H$$

ځکه دمثال په ډول که $a = 3$ او $b = 1$ وی، بیا:

$$(3 + 1\sqrt{2}) \in \mathrm{H} \;\wedge\; (3 + 1\sqrt{2}) \neq 0$$

$$\frac{a}{a^2 - 2b^2} = \frac{3}{3^2 - 2} = \frac{3}{9 - 2} = \frac{3}{7} \notin \mathbb{Z}$$

$$\frac{(-b)}{a^2 - 2b^2} = \frac{-1}{3^2 - 2} = \frac{-1}{7} \notin \mathbb{Z}$$

وموليدل چې د $(3 + 1\sqrt{2})$ لپاره په H کی معکوس وجود نه لري . پس فرعی ساحه نشی کیدای

مثال 7.2: پر F:={0,1,a,b} سیت باندی دوه دوه دوگونی رابطی په لاندي جدول کی تعریف شوي دي:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

.	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

F(+,.) یو ساحه (Field) ده چي عینت عنصریی "0„ ، واحد عنصریی "1„ او characteristic (مشخصه) یی مساوی 2 ده. ځکه:

$2.1 = 1 + 1 = 0 \quad \Rightarrow char(F) = 2$

د S:={0,1} فرعی سیت یوه فرعی ساحه (subfield) د F ده

مونږ د $p(x) = x^2 + x + 1$ پولینوم په نظرکی نیسو

که $p(x) \in F[x]$ وی، بیا کولای شودا پولینوم په دولاندي فکتوروتجزیه کړو :

$$p(x) = x^2 + x + 1 = x^2 + (a + b)x + ab = (x + a).(x + b)$$

ځکه د جدول مخی $a + b = 1$ او $a.b = 1$ کیږي. پولینوم لاندي حل لري :

$$p(x) = x^2 + x + 1 = (x + a).(x + b) = 0$$

$\Rightarrow x_1 = - a = a \ \wedge \ x_2 = -b = b$ [دجدول له مخی]

امتحان:

$$p(a) = a^2 + a + 1 = b + a +1 = 1+ 1 = 2 = 0$$
$$p(b) = b^2 + b + 1 = a + b +1 = 1+ 1 = 2 = 0$$

مگر p(x) په S[x] حل نه لری

نظر "." یو دورانی گروپ دی. ځکه: G ={1,a,b} ⊂F

$a^2 = b\ ,\ a^3 = b.a = 1 \Longrightarrow <a> = G\ \wedge ordG = 3$

$b^2 = a\ ,\ b^3 = a.b = 1 \Longrightarrow <b> = G\ \wedge ordG = 3$

لیما 7.1 : هر integeral Domain چې معین وي یو ساحه (field) ده .

ثبوت : که (D , + ,.) یو معین integ-Dom د واحد "1" عنصرسره وي.
باید ثبوت شي :

$\forall r \in D\ , r \neq 0 \Rightarrow \exists s \in D; r.s = 1$

یعني هر عنصر د D چې خلاف د صفر وي باید نظر "." ته معکوس ولري. د ثبوت لپاره د $r\in D \neq 0$ لپاره لاندي تابع په نظرکي نیسو:

$$\varphi_r\ : D \to D$$
$$x \to rx$$

: φ_r $injective$

$x, y \in D\ , \varphi_r(x) = \varphi_r(y)$

$\Rightarrow r.x = r.y \Rightarrow x = y$ [ځکه $integ - Dom$ اختصارپذیردی]

څرنګه چې D یومعین ست دی. پس د 0.1 قضیی له مخې φ_r یو surjective هم دی. پس :

$1 \in D\ \Rightarrow\ \exists\ s \in D; \varphi_r(s) = r.s = 1$

$\Rightarrow s = r^{-1} \Rightarrow r\ invertible$ [معکوس پذیر]

$\Rightarrow D\ is\ \ a\ field$ (ساحه)

لیما 7.2 : (F,+,.) یو Field او I یو ادیال په F کې دی . بیا I = {0} اویا I = F دی .

ثبوت : مونږ فرضووچې $I \neq \{0\}$ دی.

$I \neq 0\ \ \Rightarrow a \in I\ ; a \neq 0$

$\Rightarrow \exists b \in F\ \ ;\ \ a.b = 1$ [ځکه F یوه ساحه ده]

$\Rightarrow$ a invertible

$\Rightarrow I = F$ [د 6.5 لیما له مخې]

قضیه 7.1: د $(\mathbb{Z}_p, +, .)$ په رینګ کې لاندي افاده صدق کوي :

$$p\ is\ prime\ (\text{لمړنی عدد}) \Leftrightarrow \mathbb{Z}_p\ is\ field$$

ثبوت "⇒" مونږ. پوهیږو چې $(\mathbb{Z}_p,+,.)$ یو تبدیلی رینګ دی او "$\bar{1}$ " یی واحدعنصر دی. پس کفایت کوي ثبوت شي چې د هر خلاف د صفرعنصررلپاره په $\mathbb{Z}_p$ کې معکوس (inverse) موجود دی .

$$\mathbb{Z}_p = \{ \bar{0}, \bar{1}, \bar{2}, \dots , \overline{p-1} \}$$

$$\bar{a} \in {\mathbb{Z}_p}^* \Rightarrow a \in \{1,2,\dots,p-1\} \Rightarrow \gcd(a,p) = 1$$

$$\Rightarrow \exists\, x, y \in \mathbb{Z};\ a.x + p.y = 1 \quad [\,Euclidcan\ algorithm\ ]$$

$$\Rightarrow \bar{1} = \overline{a.x + p.y} = \overline{ax} + \overline{py} = \bar{a}\,.\bar{x} + \bar{p}.\bar{y}$$

$$= \bar{a}\,.\bar{x} + \bar{0}.\bar{y} = \bar{a}\,.\bar{x}$$

ولیدل شوچې $\bar{x}$ معکوس (inverse) د $\bar{a}$ دی . په نتیجه کې $\mathbb{Z}_p$ یوه ساحه ده .
اویا د 3.22 قضیی له مخې څرنګه چې p یو اولیه عدد دی. پس $(\mathbb{Z}_p^{\ *}\ ,.)$ یو ګروپ دی. یعنې د هر خلاف د صفر عنصر ته په $\mathbb{Z}_p$ کې معکوس (inverse) موجود دی.
"⇐" که p لمړنی عدد نه وي. پس باید :

$$\exists\, m,n \in \mathbb{N}\,; 1 < m\ ,\ n < p\ ,\ p = m.n$$

$$\Rightarrow (\bar{m}.\bar{n} = \overline{m.n} = \bar{p} = \bar{0}) \wedge (\bar{m} \neq \bar{0} \ \wedge\ \bar{n} \neq \bar{0})$$

$$\Rightarrow \mathbb{Z}_p \ \ is\ not\ integral\ Doman$$

$$\Rightarrow \mathbb{Z}_p \ \ is\ not\ field \quad (\text{ساحه نه ده})$$

مګر دا خلاف د فرضیی دی. پس p یو اولیه عدد دی .

قضیه 7.2 : هره ساحه (Field **)** یو Integral Domain دی.

ثبوت : که (F,+,.) یوه ساحه وي. پس F یو تبدیلی رینګ د „ 1 „ واحد عنصرسره هم دی. فقط باید ثبوت شي چې دالاندي افاده صدق کوي

$$a,b \in F,\ a \neq 0 \ \wedge\ a.b = 0 \ \Rightarrow\ b \neq 0$$

$$a,b \in F,\ a \neq 0 \ \wedge\ a.b = 0 \Rightarrow \exists\, a^{-1} \in F\ ;\ a^{-1}.a = 1$$

$b = 1.b = (a^{-1}.a).b = a^{-1}.(a.b) = a^{-1}.0 = 0$

په همدي ترتیب کولای ثبوت کړو چې که $b \neq 0$ وې. بیا $a = 0$ لاس ته راځي. په نتیجه کې F یو Integral Domain دی.

لیما 7.3: (R,+,.) یو رینګ چې عینت عنصر "0"، (F,+,.) یوه ساحه (field) چې واحدعنصر "1" او $\varphi: F \longrightarrow R$ یو R-Hom دی. بیا:

(1) φ سورجیکتیف $\Longleftarrow$ $\varphi(1)$ واحد (unity) عنصر د R دی

(2) φ بایجکتیف $\Longleftarrow$ R یوه ساحه (field) ده

(1) ثبوت:

$s \in R \Longrightarrow \exists\, a \in F\ ;\ s = \varphi(a)$ [ځکه φ یو surjective]

$\Longrightarrow s = \varphi(a) = \varphi(1.a) = \varphi(1).\varphi(a) = \varphi(1).s$

په نتیجه کی $\varphi(1)$ واحد عنصر د R دی

(2) ثبوت: په (1) کی موولیدل چې $\varphi(1)$ واحد عنصر د R دی

$\varphi(1) \neq 0$**:** که داسی نه وی بیا :

$\varphi(1) = 0 = \varphi(0) \Longrightarrow 1 = 0$ [ځکه φ یو injective]

دا امکان نه لری. ځکه په یوه ساحه کی عینیت عنصر او واحد مساوی کیدای نشي

د R **د** ساحه توب لپاره باید ثبوت شی:

(a) R نظر ".„ تبدیلی خاصیت لري

(b) هرعنصر(element) خلاف د صفرپه R کی باید معکوس ولری . یعنې:

$x \in R\ ,\ x \neq 0 \Longrightarrow \exists\, y \in R\ ;\ x.y = \varphi(1)$

(a) **ثبوت:**

$x,y \in R$

$\Longrightarrow \exists\, a,b \in F\ ;\ x = \varphi(a) \wedge y = \varphi(b)$ [ځکه φ یو surjective]

$\Longrightarrow x.y = \varphi(a).\varphi(b) = \varphi(a.b) = \varphi(b.a)$ [ځکه Fتبدیلی خاصیت لري]

$= \varphi(b).\varphi(a) = y.x$

په نتیجه کی R تبدیلی خاصیت لری

(b) **ثبوت:** په (1) کی مووليدل چې $\varphi(1)$ واحد عنصراوخلاف د صفردی

x∈ R , x≠ 0 $\Longrightarrow \exists$ a ∈ F , x = φ(a) [surjective يو φ ځکه]

$\varphi(0)$ = 0 ≠ x = $\varphi(a)$ [R-Hom يو φ ځکه]

$\Longrightarrow$ a ≠ 0 [injective يو φ ځکه]

$\Longrightarrow$ $\exists\ a^{-1} \in F$; a.a^{-1} = 1 [field يو F ځکه]

x. $\varphi(a^{-1})$ = $\varphi(a^{-1}).x$ [تبديلی خاصيت لري F ځکه]

= $\varphi(a^{-1}).\varphi(a)$ = $\varphi(a^{-1}.a)$ = $\varphi(1)$

په (1) کی مووليدل چې $\varphi(1)$ واحد عنصرد R دی. پس $\varphi(a^{-1})$ معکوسد x دی. په نتيجه کی ثبوت شوچې R يوه ساحه ده

تمرين 7.2:

R: = $\{A \in M(2x2,\mathbb{R}) \,|\, A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\}$

په 6.3 مثال کی مووليدل چې (.,+, R) يو رينګ دی. مونږدالاندي تابع لرو

$\varphi: (\mathbb{C},+,.) \longrightarrow (R,+,.)$

$z = a+ib \longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

ثبوت کړی چې (. ,+,R) يوه ساحه ده

تمرين 7.3: F:= {0,1} ⊂ ℤ

⊕	0	1
0	0	1
1	1	0

⊙	0	1
0	0	0
1	0	1

ثبوت کړی چې (⊙ , ⊕ ,F) نظر پورتنی جدول ته يوه ساحه ده

اتم فصل

Field Extensions
(ساحه یی توسعه)

تعریف 8.1: Field extensions (ساحه یی توسعه)

K یوه ساحه او $F \subseteq K$ یو فرعی ساحه (subfield) د K ده. K د F د extension field (توسعه یا تمدیده ساحه) په نوم یادیږی. مونږ هغه په K/F سره ښیو. K/F ته field extension (ساحه یی توسعه) وای
مونږد extension field پرځاي e-field اود field extension پرځاي f-extens هم لیکو.

مثال 8.1: مونږ د ناطقو اعدادو سیټ په $\mathbb{Q}$ ، دحقیقی اعدادو په $\mathbb{R}$ اود موهومی اعدادو (یا مختلط) په $\mathbb{C}$ ښودلی دی. همدارنګه پوهیږو چه $(\mathbb{Q}, +, .)$ ، $(\mathbb{R}, +, .)$ او $(\mathbb{C}, +, .)$ ساحی دي .

(a) همدارنګه $\mathbb{C}$ یو extension (توسعه) د $\mathbb{R}$ او $\mathbb{R}$ یو توسعه د $\mathbb{Q}$ دی او $\mathbb{C}/\mathbb{R}$ ،$\mathbb{R}/\mathbb{Q}$ ساحه یی توسعه (field extension) دي

(b) د $\mathbb{Q}(\sqrt{2})$ او $\mathbb{Q}(\sqrt[3]{2})$ سیټونه په لاندي ډول تعریف شوی دي:

$$\mathbb{Q}(\sqrt{2}) := \{ a+b\sqrt{2} \mid a,b \in \mathbb{Q} \},$$

$$\mathbb{Q}(\sqrt[3]{2}) := \{ a+b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q} \}$$

په اسانی سره ثبوت کولای شو چه ($\mathbb{Q}(\sqrt{2})$ او $\mathbb{Q}(\sqrt[3]{2})$ نظر جمع اوضرب ته ساحي (fields) دي. څرنګه چه $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ و $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ دي ، پس $\mathbb{Q}(\sqrt{2})$ او $\mathbb{Q}(\sqrt[3]{2})$ extension (توسعه) د $\mathbb{Q}$ دي او $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ فیلد اکستینژن (field extension) جوړوي

(c) د $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ سیټ په لاندي ډول تعریف شوی دی:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) := \{ x+y\sqrt{3} \mid x,y \in \mathbb{Q}(\sqrt{2}) \}$$

څرنګه چه x او y شامل $\mathbb{Q}(\sqrt{2})$ دي ، پس د $\mathbb{Q}(\sqrt{2})$ تعریف له مخي لیکلی شو:

$$x \in \mathbb{Q}(\sqrt{2}) \Longrightarrow \exists\, a, b \in \mathbb{Q} \,;\, x = a + b\sqrt{2}$$
$$y \in \mathbb{Q}(\sqrt{2}) \Longrightarrow \exists\, c, d \in \mathbb{Q} \,;\, y = c + d\sqrt{2}$$

په نتیجه کی:

$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{ x+y\sqrt{3} \mid x,y \in \mathbb{Q}(\sqrt{2}) \}$
$= \{ a+b\sqrt{2} + (c+d\sqrt{2}).\sqrt{3} \mid a,b,c,d \in \mathbb{Q} \}$
$= \{ a+b\sqrt{2}+c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Q} \}$

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ نظر جمع اوضرب ته هم یوه ساحه (field) ده.

څرنګه چه $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ ، پس $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ یو فیلد اکستینژن (field extension) دي

(d) $s \in \mathbb{Q}$

$\mathbb{Q}(\sqrt{s},-\sqrt{s}) = \mathbb{Q}(\sqrt{s})$

حل:

$\mathbb{Q}(\sqrt{s},-\sqrt{s}) = \{ a+b\sqrt{s} - c\sqrt{s} + d\sqrt{s.s} \mid a,b,c,d \in \mathbb{Q} \}$
$= \{ a+b\sqrt{s} - c\sqrt{s} + d.s \mid a,b,c,d \in \mathbb{Q} \}$
$= \{ (a+d.s)+(b-c)\sqrt{s} \mid a,b,c,d \in \mathbb{Q} \}$
$= \mathbb{Q}(\sqrt{s})$

(e) د $\mathbb{Q}(\sqrt{3},i)$ سیت په لاندي ډول تعریف شوی دی :

$\mathbb{Q}(\sqrt{3},i) := \{ x+yi \mid x,y \in \mathbb{Q}(\sqrt{3}) \}$

څرنګه چه x او y په $\mathbb{Q}(\sqrt{3})$ شامل دي ، پس د $\mathbb{Q}(\sqrt{3})$ تعریف له مخي لیکلی شو:

$x \in \mathbb{Q}(\sqrt{3}) \Longrightarrow \exists\, a,b \in \mathbb{Q}\,;\, x = a + b\sqrt{3}$
$y \in \mathbb{Q}(\sqrt{3}) \Longrightarrow \exists\, c,d \in \mathbb{Q}\,;\, y = c + d\sqrt{3}$

په نتیجه کی:

$\mathbb{Q}(\sqrt{3},i) = \{ x+yi \mid x,y \in \mathbb{Q}(\sqrt{3}) \}$
$= \{ a+b\sqrt{3} + (c+d\sqrt{3}).i \mid a,b,c,d \in \mathbb{Q} \}$
$= \{ a+b\sqrt{3}+ci + d\sqrt{3}\,i \mid a,b,c,d \in \mathbb{Q} \}$

$\mathbb{Q}(\sqrt{3},i)$ نظر جمع اوضرب ته هم یوه ساحه (field) ده. د i معکوس د تعریف له مخي i– دی. ځکه: $i.(-i) = -i^2 = -(-1) = 1$

څرنګه چه $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3},i)$ صدق کوي، پس $\mathbb{Q}(\sqrt{3},i)$ توسعه فیلد (extension field) د $\mathbb{Q}$ دی. یعنی: $\mathbb{Q}(\sqrt{3},i)/\mathbb{Q}$

(f) د $\mathbb{Q}(i)$ سیت په لاندي شکل تعریف شویدی:

$\mathbb{Q}(i) := \{ x+yi \mid x,y \in \mathbb{Q} \}$

خرنگه چه $\mathbb{Q}(i)$ ، $\mathbb{Q} \subseteq \mathbb{Q}(i)$ پس $\mathbb{Q}(i)$ توسعه فیلد (extension field) د $\mathbb{Q}$ دی. یعنی: $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$

تبصره 8.1: که مونږیو field extension (ساحه یی توسعه) K/F ولرو، بیا K یو وکتوری فضای نظر F ته ده.ځکه لاندي دوه ګوني رابطي صدق کوي:

$$+: K \times K \longrightarrow K$$
$$(u, v) \longmapsto u + v$$
$$\cdot: \ F \times K \longrightarrow K$$
$$(\tau, v) \longmapsto \tau v$$

او K نظر دی دو رابطوته لاندي خاصیتونه لري :

(v_1) $(K, +)$ یو تبادلوی (Commutative) ګروپ دی . عینیت عنصریي صفر ، چه مونږ هغه په " 0" سره ښیو او$-v$ معکوس (inverse) د v دی

(v_2) : د v , $v_1, v_2 \in K$ او τ , $\tau_1, \tau_2 \in F$ لپاره لاندي افادي صدق کوی:

I. $(\tau_1 + \tau_2)v = \tau_1 v + \tau_2 v$

II. $\tau(v_1 + v_2) = \tau v_1 + \tau v_2$

III. $\tau_1(\tau_2 v) = (\tau_1 \tau_2)v$

IV . $1. v = v$

په نتیجه کي K یوه وکتوری فضای نظر F ته ده او مونږهغه په (K,F) سره ښیو

تعریف 8.2 : degree of field extension

مونږ K/F لرو. دهغه وکتوری فضای په (K,F) ښیو. د (K,F) بعد (Dimension) د degree of field extension (ساحه یی توسعي درجه) په نوم یادیږي اومونږهغه په [K:F] سره ښیو. یعنی:

$$\dim(\mathrm{K,F}) = [\mathrm{K:F}]$$

که [K:F] متناهی وي ، بیا K د finite field extension نظرF په نوم یادوي

مثال 8.2:

(a) مونږد $\mathbb{C}/\mathbb{R}$ په نظرکی نیسو. {1,i} د ($\mathbb{C}, \mathbb{R}$) وکتوری فضا قاعده ده. ځکه:

$$\mathbb{C} = \mathbb{R} + \mathbb{R}i$$

یعنی د $\mathbb{C}$ هروکتورکولای شود 1 او i د خطی ترکیب بشکل ولیکو .علاوه پرهغه دوي خطی مستقل هم دي.

په نتیجه کی {1,i} یوه قاعده د ($\mathbb{C}, \mathbb{R}$) ده. پس درجه د $\mathbb{C}/\mathbb{R}$ مساوی به 2 ده.
یعنی: $[\mathbb{C}:\mathbb{R}] = 2$

(b) د $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ درجه (degree) مساوی په 2 ده.

حل: په پورته مثال کی موولیدل چه $\mathbb{Q}(\sqrt{2})$ دساحه يي توسعه (field extension) د $\mathbb{Q}$ دی. پس ($\mathbb{Q}(\sqrt{2}), \mathbb{Q}$) یوه وکتوری فضا هم ده.
ځرنګه چه $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2}$ تعریف شویدی، پس کولای شو هروکتور د $\mathbb{Q}(\sqrt{2})$ د 1 ، $\sqrt{2}$ د خطی ترکیب په بشکل ولیکو. علاوه پرهغه 1 ، $\sqrt{2}$ خطی مستقل هم دي. پس { $1, \sqrt{2}$ } یوه قاعده د ($\mathbb{Q}(\sqrt{2}), \mathbb{Q}$) ده.
په نتیجه کی:

$$\dim((\mathbb{Q}(\sqrt{2}),\mathbb{Q})) = 2 \implies [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$$

(c) د $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ درجه (degree) 4 ده.
حل: د $\mathbb{Q}(\sqrt{2},\sqrt{3})$ سیت په لاندي شکل تعریف شویدی:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{ a+b\sqrt{2}+c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Q} \}$$

په پورتني مثال کی موولیدل چه $\mathbb{Q}(\sqrt{2},\sqrt{3})$ ساحه یی توسعه (f- extens) د $\mathbb{Q}$ دی. پس ($\mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}$) یووکتوری فضا هم ده.
د $\mathbb{Q}(\sqrt{2},\sqrt{3})$ هروکتورد { $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ } خطی ترکیب په شکل لیکل کیدای شي. علاوه پرهغه خطی مستقل هم دي. پس { $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ } یوه قاعده د ($\mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}$) ده. په نتیجه کی:

$$\dim(\mathbb{Q}(\sqrt{2},\sqrt{3}),\mathbb{Q}) = 4 \implies [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$$

(d) د $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$ درجه (degree) 4 ده.
حل: د $\mathbb{Q}(\sqrt{3}, i)$ سیت په لاندي شکل تعریف شویدی:

$$\mathbb{Q}(\sqrt{3}, i) := = \{ a+b\sqrt{3}+ci + d\sqrt{3}\, i \mid a,b,c,d \in \mathbb{Q} \}$$

په پورتني مثال کی موولیدل چه $\mathbb{Q}(\sqrt{3}, i)$ یو field extension د $\mathbb{Q}$ دی. پس ($\mathbb{Q}(\sqrt{3}, i), \mathbb{Q}$) یو فضای وکتور هم دی.
د $\mathbb{Q}(\sqrt{3}, i)$ هروکتورد { $1, \sqrt{3}, i, \sqrt{3}i$ } خطی ترکیب په شکل لیکلی شو.
علاوه په هغه خطی مستقل هم دي. پس { $1, \sqrt{3}, i, i\sqrt{3}$ } یوه قاعده د ($\mathbb{Q}(\sqrt{3}, i), \mathbb{Q}$) ده. په نتیجه کي:

$\dim(\mathbb{Q}(\sqrt{3},i),\mathbb{Q})\ ) = 4 \implies [\mathbb{Q}(\sqrt{3},i):\mathbb{Q}] = 4$

(e) د $\mathbb{Q}(\sqrt[3]{2})\ //\ \mathbb{Q}$ درجه (degree) 3 ده.

حل: د $\mathbb{Q}(\sqrt[3]{2})$ سیت په لاندي شکل ذیل تعریف شویدی:

$\mathbb{Q}\ (\sqrt[3]{2}\ ) := \{\ a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c\ \in \mathbb{Q}\ \}$

پورتني مثال کی مووليدل چه $\mathbb{Q}(\sqrt[3]{2})$ يوساحه يي توسعه (field extension) د $\mathbb{Q}$ دی. پس $(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})$ يو وکتوری فضا هم ده. د تعریف له مخی هروکتورد $\mathbb{Q}\ (\sqrt[3]{2})$ د $\{1, \sqrt[3]{2}, \sqrt[3]{4}\ \}$ د خطی ترکيب په شکل ليکلی شو. علاوه پرهغه خطی مستقل هم دی. پس $\{\ 1, \sqrt[3]{2}, \sqrt[3]{4}\ \}$ يوه قاعده $(\mathbb{Q}(\sqrt[3]{2}\ ),\mathbb{Q})$ ده.

په نتيجه کی :

$\dim(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})\ ) = 3 \implies [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$

(f) مونږ توسعه فیلد $\mathbb{Q}(\mathrm{i}\ )\ /\ \mathbb{Q}$ په نظرکی نيسو. د $(\mathbb{Q}(\mathrm{i}\ ),\mathbb{Q})$ وکتوری فضا قاعده {1,i} ده.ځکه هروکتور د $\mathbb{Q}(\mathrm{i}\ )$ يو خطی ترکيب د 1 ، i وکتورو دی.
علاوه پرهغه خطی مستقل هم دی.
وښودل شوچه {1,i} يوه قاعده د $(\mathbb{Q}(\mathrm{i}\ ),\mathbb{Q})$ ده. پس د $\mathbb{Q}(\mathrm{i}\ )/\mathbb{Q}$ درجه 2 ده. يعنی: $[\mathbb{Q}(\mathrm{i}\ ):\mathbb{Q}] = 2$

مثال8.3 :

$\mathbb{Q}\ (\sqrt{6}) := \{\ a+b\sqrt{6} \mid\ a,b\ \in \mathbb{Q}\ \} \Longrightarrow [\mathbb{Q}(\sqrt{6}):\mathbb{Q}]\ = 2$

$[\mathbb{Q}(\sqrt[n]{q}):\mathbb{Q}] = \mathrm{n}$ (پدی شرط چه q يو اوليه عدد وي)

تمرين 8.1:

(1) ثبوت کړی چه $(\mathbb{Q}(\sqrt{5}\ ),+,.)$ يوه ساحه (field) ده.

(2) ثبوت کړی چه $\mathbb{Q}$ فرعی سيت (subset) د $\mathbb{Q}(\sqrt{5}\ )$ دی.

يعنی: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}\ )$

(3) د $(\mathbb{Q}(\sqrt{5}\ ),\mathbb{Q})$ وکتوری فضا قاعده (basis) پيداکړی.

(4) د $\mathbb{Q}(\sqrt{5}\ )/\ \mathbb{Q}$ وکتوری فضا درجه (degree) ځوده

تمرين 8.2:

(1) ثبوت کړی چه $(\mathbb{Q}(\sqrt{3}\ ,\sqrt{5}\ ),+,.)$ يوه ساحه (field) ده.

(2) ثبوت کړی چه $\mathbb{Q}(\sqrt{3}\ ,\sqrt{5}\ )/\mathbb{Q}$ يو (field extension) دی

(3) د $(\mathbb{Q}(\sqrt{3}\ ,\sqrt{5}\ ),\mathbb{Q})$ وکتوری فضا يوه قاعده (basis) پيداکړی.

(4) د $(\mathbb{Q}(\sqrt{3}\ ,\sqrt{5}\ ))/\ \mathbb{Q}$ درجه (degree) ځوده

تعریف8.3 : K/F یو field extension (ساحه يي توسعه) دی. یو $\alpha \in K$ د
الجبری نظر F (algebraic over F) په نوم یادیږی، پدی شرط چه یوه پولینوم
p(x) $\in F[x]$ خلاف دصفرموجوده وي ، چه p(α) = 0 شی. که چیری
داحالت موجود نه وی، بیا α د transcendental (تخیلی) په نوم یادیږی. یعنی
p(α) = 0 فقط هغه وخت صدق کوی، چه p صفری پولینوم وي. مونږد K
الجبری عناصرو سیت به $\mathbb{A}$ سره ښیو. د مثال په ډول:

$\mathbb{A} := \{\alpha \in K \mid \exists\, \mathrm{p(x)} \in F[x]; p \neq 0 \ \wedge\ \mathrm{p}(\alpha) = 0\}$

$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \exists\, \mathrm{p(x)} \in \mathbb{Q}[x]; p \neq 0 \ \wedge\ \mathrm{p}(\alpha) = 0\}$

$= \{\alpha \in \mathbb{C}\ |$ ته $\mathbb{Q}$ الجبری خاصیت نظر $\alpha\}$

البته د $F[X]$ سیت چه په 6.12 تعریف کی تشریح شوی وه ،یورینګ (ring)
هم دی.

تبصره : دیوی ساحي F هرعنصر نظر خپله F ته الجبري دی. ځکه:

$\forall\alpha \in F, \exists\, \mathrm{p}(x) = x - \alpha \in F[x]\,; \mathrm{p}(\alpha) = 0$

مثال 8.4 : مونږد $\mathbb{C}/\mathbb{R}$ ساحه يي توسعه په نظرکی نیسو .

$\alpha := 2+3i \in \mathbb{C}$

$$\begin{aligned}(x-\alpha).(x-\bar{\alpha}) &= (x-(2+3i)).(x-(2-3i))\\ &= (x-2-3i).(x-2+3i)\\ &= x^2 - 2.2x + (2^2+3^2)\\ &= x^2 - 4x + 13 \in \mathbb{R}[x]\end{aligned}$$

$\mathrm{p}(x) := x^2 - 4x + 13$

$\mathrm{p}(\alpha) = \alpha^2 - 4\alpha + 13 = (2+3i).(2+3i) - 4(2+3i) + 13$

$= 4+6i+6i-9-8-12i+13 = 0$

پس یو پولینوم p(x) په $\mathbb{R}[x]$ کی پیدا شوچه p(α) = 0 دی او په نتیجه کی
α = 2+3i یو الجبری (algebraic) عنصرنظر $\mathbb{R}$ ته دی.

مثال 8.5 : مونږد $\mathbb{R}/\mathbb{Q}$ ساحه يي توسعه په نظرکی نیسو

(a) حقیقی عدد $\sqrt[3]{2}$ نظر $\mathbb{Q}$ ته الجبری دی. ځکه:

$P(x) = x^3 - 2 \in \mathbb{Q}[X] \ \wedge\ p(\sqrt{2}) = (\sqrt[3]{2})^3 - 2 = 2 - 2 = 0$

د $\sqrt[3]{2}$ لپاره یو پولینوم P(x) پیداشوه چه $\sqrt[3]{2}$ دهغه جذردی.

(b) حقیقی عدد $\sqrt{2}$ نظر $\mathbb{Q}$ ته الجبری دی. ځکه :

$\mathrm{p}(x)\!: x^2 - 2 \in \mathbb{Q}[X] \ \wedge\ \mathrm{p}(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$

π = 3.14159.... او e= 2.71828.... عدودنه په $\mathbb{R}/\mathbb{Q}$ کی
transcendental دي. ځکه نشوکولای یوپولینوم $p(x) \in \mathbb{Q}[x]$ پیدا کړو چه

$p(e) = 0$ شی. مگر $\mathbb{C}/\mathbb{R}$ دا اعداد الجبری (algebraic) نظر $\mathbb{R}$ ته دي.
ځکه:

$P_1(x) := x - e \in \mathbb{R}[x]$, $P_2(x) := x - \pi \in \mathbb{R}[x]$
$P_1(e) := e - e = 0$, $P_2(\pi) := \pi - \pi = 0$

تعریف 8.4:
(a) یو ساحه یي توسعه K/F د algebraic (الجبری) په نوم یادیږی، پدي شرط چه هر $\alpha \in K$ الجبری نظر F (algebraic over F) ته وی او K په نوم د algebraic extension د F یادیږی . یعنی :

$\forall \alpha \in K \implies \exists\, p \in F[X] ; p \neq 0 \wedge p(\alpha) = 0$

په غیردهغه K/F د transcendental په نوم یادیږی
(b) یو فیلد F ته algebraic closure ویل کیږی، که چیری:

$\forall\, p(x) \in F[X] , \deg(p(x)) > 0 \implies \exists\, a \in F ; p(a) = 0$

(یعنی هرپولینوم په $F[X]$ کی چه درجه یی صفر نه وی، په F کی اقلاً یو جذر لری)

مثال 8.6 : ساحه یي توسعه $\mathbb{C}/\mathbb{R}$ الجبری (algebraic) دی. ځکه:

$\alpha: a+ib \in \mathbb{C}$
$(x - \alpha) . (x - \bar{\alpha}) = (x - (a+ib)).(x - (a - ib))$
$= x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[X]$
$p(x) := x^2 - 2ax + (a^2 + b^2)$
$p(\alpha) = \alpha^2 - 2a\,\alpha + a^2 + b^2 = (a + ib)^2 - 2a(a + ib) + a^2 + b^2$
$= a^2 + 2aib - b^2 - 2a^2 - 2aib + a^2 + b^2 = 0$

ولیدل شوچه دهر $\alpha \in \mathbb{C}$ لپاره یو پولینوم p(x) په $\mathbb{R}[X]$ کی پیدا شوچه $p(\alpha) = 0$ دی. پس $\mathbb{C}/\mathbb{R}$ الجبری (algebraic) دی

لیما 8.1: K او F ساحی دي.

K/F finite (متناهی) $\implies$ K/F algebraic

ثبوت: خرنګه چه K/F متناهی دی، پس مونږ فرض کوچه:

n:= [K:F]= dim(K,F)

یعنی د K فضای وکتورد قاعدی (basis) دوکتوروشمیر n دی. داپدي معنی چه دخطی مستقل (linearly independet) وکتورو شمیرپه K کی له n څخه زیات کیدای نشی. پس د یو $\alpha \in K$ لپاره $\{ 1, \alpha, \alpha^2 , \alpha^3, \ldots , \alpha^n\}$ وابسته خطی (lin-dep) دي

$1, \alpha, \alpha^2 , \alpha^3, \ldots , \alpha^n$ (lin-dep)

$\implies \exists\, a_0,a_1,a_2,\ldots,a_n \in F$ (not all zero);
$a_0 + a_1 \alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$

$\Longrightarrow$ α algebraic
$\Longrightarrow$ K/F algebraic

قضیه 8.1: (theorem of Lagrange for fields)

که K/T او T/F دوه متناهی ساحه يي توسعه (finite field extensions) وي ، بيا:

$[K:F] = [K:T] . [T:F]$

ثبوت: مونږد K وکتوری فضای بعد نظر T ته په m اود T نظر F ته په n ښيو. يعنی:

$\dim(K,T) = m \;\wedge\; \dim(T,F) = n$

اويا داچه:

$[K:T] = m \;\wedge\; [T:F] = n$

که $\{u_m, \ldots, u_3, u_2, u_1\}$ يوه قاعده (basis) د K او $\{v_n, \ldots, v_3, v_2, v_1\}$ يوه قاعده (basis) د T وي،بيا:

$u \in K \Longrightarrow \exists\, a_1, a_2, \ldots, a_m \in T$;

$$u = a_1u_1 + a_2 u_2 + \ldots + a_mu_m = \sum_{i=1}^{m} a_i . u_i$$

$a_i \in T \Longrightarrow \exists\, b_{i1}, b_{i2}, \ldots, b_{in} \in F$;

$$a_i = b_{i1}v_1 + b_{i2} v_2 + \ldots + b_{in}v_n \quad (i=1,2,\ldots,m)$$
$$= \sum_{j=1}^{n} b_{ij}\, v_j$$

$$\begin{aligned} u &= (b_{11}v_1 + b_{12} v_2 + \ldots + b_{1n}v_n).u_1 \\ &\quad + (b_{21}v_1 + b_{22} v_2 + \ldots + b_{2n}v_n).u_2 \\ &\quad + \ldots\ \ldots\ldots + \\ &\quad + (b_{m1}v_1 + b_{m2} v_2 + \ldots + b_{mn}v_n).u_m \\ &= (b_{11}v_1.u_1 + b_{12} v_2 .u_1 + \ldots + b_{1n}v_n .u_1) \\ &\quad + (b_{21}v_1.u_2 + b_{22} v_2 .u_2 + \ldots + b_{2n}v_n .u_2) \\ &\quad + \ldots\ldots\ldots\ldots + \\ &\quad + (b_{m1}t_1.k_m + b_{m2} t_2 .k_2 + \ldots + b_{mn}t_n .k_m) \\ &= \sum_{i=1}^{m} a_i . u_i = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n} b_{ij}\, v_j \Big) . u_i \end{aligned}$$

وښودل شو چه لاندي وکتورونه چه شمير يی m.n ته رسيږی، د K وکتوری فضا يو span جوړوی

$$\{(u_i. v_j) \mid i = 1,1, \ldots, m \;\wedge\; j = 1,2, \ldots, n\}$$

اوس بايد ثبوت شی چه پس وکتورونه خطی مستقل هم دي.

$\sum_{i=1}^{m}\Big(\sum_{j=1}^{n} b_{ij}\, v_j \Big) . u_i = 0$

$\Longrightarrow \ \sum_{j=1}^{n} \ b_{ij} v_j = 0$ [ځکه چه u_i قاعده ده]

$\Longrightarrow b_{ij} = 0 \ \ (i = 1,1, \dots, m \ \ \wedge \ j = 1,2, \dots, n)$ [ځکه v_j قاعده]

ثبوت شوچه $\{(u_i . v_j) \mid i = 1,1, \dots, m \ \wedge j = 1,2, \dots, n\}$ یوه قاعده د K وکتوری فضا نظر F ته ده. پس:

$$\dim((K,F)) = m.n$$

$$[K:F] = m.n = [K:T] . [T:F]$$

تبصره 8.2:

(1) که مونږیوه ساحه K ولرو چي T او F د هغه فرعی ساحي (subfield) وي او $F \subseteq T \subseteq K$. بیا:

(a)

$$r := [K:F] , m := [K:T] , n := [T:F] \Longrightarrow m \mid r \ \ \wedge \ \ n \mid r$$

یعنی r پر m او n باندي قابل دتقسیم دی.

(b) که [K:F] یواولیه عدد وي، پدي نصورت بیا T ساحه د K سره مساوی اویا F سره مساوی ده. یعنی د K او F ترمینځ دکومی بلي ساحی موجودیت امکان نشته

(2)

$F_1 \subseteq F_2 \subseteq \dots \subseteq F_n \ \ \wedge \ F_{i+1}/F_i \ \ (i = 1,2,\dots,n-1)$

finite field extension (متناهی توسعه فیلد)

$$\Longrightarrow \ [F_n:F_1] = \prod_{i=1}^{n-1} [F_{i+1} : F_i \ ]$$

تعریف 8.5 :

(a) دا لاندي پولینوم د monic plynomial په نوم یادیږی، پدي شرط چه $a_n = 1$ وی

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$$

مثال په ډول دا لاندي پولینوم monic ده:

$$p(x) = x^4 + 5x^3 + 4x^2 + 3x + 6$$

(b) F یوه ساحه (field) ده. یو پولینوم $p(x) \in F[x]$ د قابل دتجزیه (reducible polynomial) په نوم یادیږي، پدی شرط چه:

(i) p(x) غیرثابته (not constant) وي. یعنی: $\deg(p(x)) \neq 0$

(ii) دوه پولینومی f(x),g(x) په $F[x]$ دلاندي خواصو سره موجودي وي:

$$\deg(f(x)) \neq 0 \wedge \deg(g(x)) \neq 0 \ \wedge \ p(x) = f(x).g(x)$$

که هغسی نه وی، بیاد irreducible polynomial (غیرقابل تجزیه) په نوم یادیږی. یعنی که یوپولینوم په غیرثابت فکتورو قابل دتجزیه وی ، د

reducible polynomial په نوم اوغیرله هغه د irreducible polynomial (غیرقابل تجزیه) په نوم یادیږي

مثال 8.7:

$P_1(x) = x^2 + 4x + 4 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$

$P_2(x) = x^2 - 4 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$

$P_3(x) = x^2 - 2 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$

$P_4(x) = x^2 + 1 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$

$P_5(x) = x^2 - \frac{4}{9} \in \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$

پورتني پولینومي کولای شوپه لاندي ډول ولیکو:

$P_1(x) = x^2 + 4x + 4 = (x + 2).(x + 2)$

$P_2(x) = x^2 - 4 = (x + 2).(x - 2)$

$P_3(x) = x^2 - 2 = (x + \sqrt{2}).(x - \sqrt{2})$

$P_4(x) = x^2 + 1 = (x + i).(x - i)$

$P_5(x) = x^2 - \frac{4}{9} = (x + \frac{2}{3}).(x - \frac{2}{3})$

$p_6(x) = x^2 + \bar{1} \in \mathbb{Z}_2[X]$

$p_2(x), p_1(x)$ په $\mathbb{Z}$ کی reducible (قابل دتجزيي) پولینومي .

مګر $p_5(x), p_4(x), p_3(x)$ په $\mathbb{Z}$ کي irreducible پولینومي دي.

$P_5(x)$ په $\mathbb{Q}$ کی reducible پولینوم ده. مګر $p_4(x), p_3(x)$ په $\mathbb{Q}$ کي irreducible پولینومي دي

$P_3(x)$ په $\mathbb{R}$ کي reducible پولینوم ، مګر $p_4(x)$ په $\mathbb{R}$ کي irreducible پولینوم ده

$p_6(x)$ په $\mathbb{Z}_2$ فیلد کی reducible (قابل دتجزیه) ده. ځکه :

$p(x) = x^2 + \bar{1} = (x + \bar{1}).(x + \bar{1})$

مثال: مونږیوه ساحه F او $p(x)= x^2 + 1 \in F[X]$ لرو. $p(x)$ په F هغه وخت قابل دتجزیه ده ، چه یو λ په F موجود وي چه $\lambda^2 = -1$ صدق وکړی. لاندي جدول ښیي چه په کومه ساحه کی $p(x)= x^2 + 1$ قابل دتجزیه ده.

Field		p(x)
$\mathbb{C}$	$\lambda = i$, $p(i) = i^2 + 1 = -1 + 1 = 0$	reducible
$\mathbb{Z}_2$	$\lambda = \bar{1}$, $p(\bar{1}) = (\bar{1})^2 + \bar{1} = \bar{1} + \bar{1} = \bar{0}$	reducible
$\mathbb{Z}_3$		irreducible
$\mathbb{Z}_5$	$\lambda = \bar{2}$, $p(\bar{2}) = (\bar{2})^2 + \bar{1} = \bar{4} + \bar{1} = \bar{0}$	reducible

تبصره 8.3: K/F یو field extension (ساحه يي توسعه) او $\alpha \in K$ یو الجبری عنصرنظر F ته دی

$$I_\alpha := \{g \in F[x] \mid g(\alpha) = 0\}$$

د I_α سیت یو Ideal په F[x] رینګ کی دی . ځکه:

$$f,g \in I_\alpha \Rightarrow f(\alpha) = 0 \wedge g(\alpha) = 0 \Rightarrow (f+g)(\alpha) = 0$$
$$\Rightarrow f+g \in I_\alpha$$
$$f \in I_\alpha ,\ g \in F[x] \Rightarrow f(\alpha) = 0 \Rightarrow f(\alpha).g(\alpha) = 0.g(\alpha) = 0$$
$$\Rightarrow f.g \in I_\alpha$$

په نتیجه کي I_α یو ایدیال په $F[x]$ دی.

هغه پولینوم چه په I_α کي تیټه درجه ولري او monic وي، د α minimal plynomial په نوم نظر F ته یادیري او مونږهغه په m_α سره ښیو. m_α پولینوم لاندي خواص لري:

(i) $I_\alpha = < m_\alpha >$

(یعنی m_α مولد د I_α ادیال)

(ii)

$$g \in I_\alpha \Rightarrow \exists f \in I_\alpha ; g = f.m_\alpha$$

(یعنی د I_α هرپولینوم پر m_α قابل د تقسیم ده)

مثال 8.8 :

(a) په K/F ساحه يي توسعه کي هر $\alpha \in K$ لاندي منیمال پولینوم لری:

$$m_\alpha(x) = x - \alpha$$

(b) په $\mathbb{C}/\mathbb{R}$ ساحه يي توسعه کی منیمال پولینوم (minimal plynomial) نظر $i \in \mathbb{C}$ ته لاندي شکل ذیل لري:

$$m_i(x) = x^2 + 1 \in \mathbb{R}[X]$$

ځکه:

$$m_i(i) = i^2 + 1 = -1 + 1 = 0$$

نور خواص هم صدق کوي

(c) مونږ $\mathbb{R}/\mathbb{Q}$ ساحه يي توسعه په نظرکي نیسو. $\sqrt{2}$ او $\sqrt[3]{2}$ حقیقی اعداد نظر $\mathbb{Q}$ ته الجبری دي. منیمال پولینوم يي (minimal plynomial) لاندي شکل لری :

$$\alpha := \sqrt{2} \quad m_\alpha(x) = x^2 - 2 \in \mathbb{Q}[X]$$
$$\alpha = \sqrt[3]{2} \quad m_\alpha(x) = x^3 - 2 \in \mathbb{Q}[X]$$

یعنی $x^2 - 2$ منیمال پولینوم د $\sqrt{2}$ نظر $\mathbb{R}$ ته او $x^3 - 2$ منیمال پولینوم د $\sqrt[3]{2}$ نظر $\mathbb{R}$ ده.

تعریف 8.6: L/F یو ساحه يي توسعه ده.

(a) (field adjunction): $S\subseteq L$

مونږ ترټولو کوچني فرعی ساحه (subfield) چه S او F په کي شامل وی، په F(S) سره ښیو. ویل کیږی چه د F(S) ساحه له F څخه د adjunction (داتحاد په معنی) په واسطه د S سیت څخه لاسته راغلی.

که $S = \{a_1,a_2,...,a_n\}$ وي، بیا مونږ $F(a_1,a_2,...,a_n)$ د F(S) پرځای او که $S = \{a\}$ وی، بیا F(a) لیکو.

مثال: په $\mathbb{R}/\mathbb{Q}$ کي د $\mathbb{Q}(\sqrt{2})$ فیلد له $\mathbb{Q}$ څخه د $\sqrt{2}$ عدد د adjunction پواسطه لاس ته راځی. ځکه :

$S:= \{\sqrt{2}\}$

$$S\subseteq \mathbb{R} \wedge \mathbb{Q}\subseteq \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(S) \subseteq \mathbb{R}$$

همدارنګه په $\mathbb{C}/\mathbb{Q}$ کي د $\mathbb{Q}(\sqrt{2},i)$ فیلد له $\mathbb{Q}$ څخه د $\sqrt{2}$ ، i اعدادو adjunction په واسطه لاس ته راغلی. ځکه د $S:= \{\sqrt{2},i\}$ لپاره:

$$S\subseteq \mathbb{C} \wedge \mathbb{Q}\subseteq \mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(S) \subseteq \mathbb{C}$$

(b) (Simple extention): L/F ساحه يي توسعه د Simple extention په نوم یادیږي ، که یو $a\in L$ موجودوي، چه F(a) = L شی.

مثال : $\mathbb{C}/\mathbb{R}$ یو Simple extention دی. ځکه د $i\in\mathbb{C}$ لپاره:

$$\mathbb{R}(i) = \{a+bi \mid a,b\in \mathbb{R}\} = \mathbb{C}$$

همدارنګه $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ یو Simple extention دی.ځکه:

$$\sqrt{2}\in\mathbb{Q}(\sqrt{2})$$

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b\in \mathbb{Q}\}$$

(c) (Splitting field): $p(x)\in F[X]$

د L ساحه د p(x) د Splitting field نظر F په نوم یادیږي، که چیري:

(i) p(x) په L کی په خطی فکتوروتجزیه شی. یعنی:

$$P(x) = c(x-a_1).(x-a_2)....(x-a_n) \ , c\in F \ , a_1, a_2,...., a_n\in L$$

(ii)

$$L = F(a_1, a_2,...., a_n)$$

تبصره 8.4: F یو فیلد دی. که $p(x)\in F[X]$ په F کی په خطی فکتوو تجزیه شی، پدی حالت کي F خپله Splitting field د P(x) دی.

مثال 8.9 :

(a)

$$p_1(x) = X - 3, \ p_2(x) = x^2 - 4 = (x+2)(x-2) \in \mathbb{Q}[X]$$

څرنګه چه $p_1(x)$ او $p_2(x)$ په $\mathbb{Q}$ کی په خطی فکتورو قابل د تجزی دي او علاوه پر هغه:

$\mathbb{Q}(3) = \{a + 3b \mid a, b \in \mathbb{Q}\} = \mathbb{Q}$
$\mathbb{Q}(2, -2) = \mathbb{Q}(2)$ [نظر په مثال (d) .8.1]
$\mathbb{Q}(2) = \{a + 2b \mid a, b \in \mathbb{Q}\} = \mathbb{Q}$
لیدل کیږي چه $\mathbb{Q}$ نظر $P_1(x)$ او $p_2(x)$ ته یوه splitting ساحه ده.

(b) مونږ $\mathbb{R}/\mathbb{Q}$ ساحه یي توسعه په نظرکی نیسو

$p(x) = x^2 - 2 \in \mathbb{Q}[X] \implies p(x) = x^2 - 2 = (x + \sqrt{2}).(x - \sqrt{2})$

څرنګه چه $\sqrt{2}, -\sqrt{2} \in \mathbb{R}$ دي، پس splitting ساحه د $\mathbb{R}$ نظر $p(x)$ ته لاندي شکل لري:

$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ [دمثال (d) .8.1 له مخي]

(c) مونږ $\mathbb{C}/\mathbb{R}$ ساحه یي توسعه په نظرکی نیسو

$p(x) = x^2 + 1 \in \mathbb{R}[X] \implies p(x) = (x + i).(x - i)$

څرنګه چه $i, -i \in \mathbb{C}$ دي، پس splitting ساحه د $\mathbb{C}$ نظر $p(x)$ ته لاندي شکل لري:

$$\mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C}$$

(d)

$p(x) = (x^2 - 2).((x^2 + 1) \in \mathbb{Q}[X]$
$p(x) = (x^2 - 2).((x^2 + 1) = (x - \sqrt{2}).(x + \sqrt{2})(x+i)(x-i)$

څرنګه چه $i, \sqrt{2} \in \mathbb{C}$ دي، پس $\mathbb{Q}(\sqrt{2}, i)$ یوه splitting ساحه د $\mathbb{C}$ نظر $p(x)$ ته ده

قضیه 8.2: (fundamental theorem of algebra)

د موهومی اعدادو ساحه $\mathbb{C}$ یوه *algebraic closure* (الجبری تړلي) ساحه ده.
یعنی هره غیرثابته تابع $p(x) \in \mathbb{C}[X]$ په $\mathbb{C}$ کي په خطی فکتوروقابل د تجزیي ده
د مثال په ډول که یوه پولینوم $p(x)$ لاندي شکل ولري:

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$

بیا اعداد $z_1, z_2, \ldots, z_n \in \mathbb{C}$ موجود دي چه:

$p(x) = a_n(x - z_1).(x - z_2)\ldots(x - z_n)$

دلته $z_1, z_2, \ldots, z_n$ د پولینوم جذرونه دي.
دا د الجبراساسی قضیه د Gauss په نوم هم یادیږي. البته ګوس دا د حقیقی اعدادو لپاره ثبوت کړیده. یعنی هرپولینوم $p(x) \in \mathbb{R}[X]$ په خطی او مربعی فکتورو تجزیه کیدلاشی.

ثبوت: له ثبوت څخه یي صرف نظر کوو.

تعریف 8.7: (quotient field) **:** مونږ Integral domain (انتګرال دومین) D لرو. یوه ساحه Q د D د quotient field په نامه یادیږي، که چیری :

(i) D یو فرعی رینګ (subring) د Q وي

(ii)

$\forall\, a \in Q \quad \exists\, r, s \in D \ ; \ a = rs^{-1} \ \ (s^{-1} \in Q)$

مونږهغه په $Q = quot(D)$ سره بنيو

مثال 8.10: د $(\mathbb{Q}, +, .)$ ساحه يو quotient field د $(\mathbb{Z}, +, .)$ دی. يعنی:

$\mathbb{Q} = quot(\mathbb{Z})$

حل: مونږپوهيږو چه $\mathbb{Z}$ يوانتګرال دومين او فرعی رينګ د $\mathbb{Q}$ دی. $\alpha \in \mathbb{Q}$

د $\alpha = 0$ دپاره واضح ده

$\alpha \neq 0 \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0 \ ; \ \alpha = \frac{a}{b}$ [نظر $\mathbb{Q}$ تعريف]

$\Rightarrow b \in \mathbb{Q} \Rightarrow \exists b^{-1} \in \mathbb{Q}$ [ځکه $\mathbb{Q}$ يوه ساحه ده]

$\Rightarrow \alpha = \frac{a}{b} = ab^{-1} \Rightarrow (ii)$

په نتيجه کي: $\mathbb{Q} = quot(\mathbb{Z})$

نوت: هره ساحه په خپله quotient field دی

تعريف 8.8: (Eisenstein's Irreducibility criterion)

Eisenstein يو المانی رياضی عالم (1852 – 1823) پيداکړ چه څه وخت يوه پولينوم irreducible (غير قابل د تجزيی) ده. D يوانتګرال دومين او Q يوه quotient ساحه دهغه ده.يعنی: $Q = quot(D)$. مونږلاندي پولينوم لرو :

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in D[X]\ ,\ a_n \neq 0\ ,\ n > 1$

Eisenstein **واي:**

د $f(x)$ پولينوم **هغه وخت** irreducible (دتجزيي وړنه) ده ، که چيري يو لمړنی عنصر (primelement) $p \in Q$ دلاندي خواصوسره موجود وي:

(i) $\quad p \nmid a_n$ (يعنی a_n پر p بانه دي قابل د تقسيم نه وي)

(ii) $\quad p \mid a_i \quad (i = 0,1,2,\dots, n-1)$

(iii) $\quad p^2 \nmid a_0$ (يعنی a_0 پر p^2 بانه دي قابل د تقسيم نه وي)

نوت:دثبوت څخه يی فعلاً صرف نظرکوو.

مثال 8.11:

(a) مونږوليدل چه $\mathbb{Q} = quot(\mathbb{Z})$ دی

$f(x) = x^3 + 9x^2 + 6x - 3 \in \mathbb{Z}[X]$

پدي مثال کي

$a_3 = 1, a_2 = 9, a_1 = 6, a_0 = -3$

$p = 3$ يو اوليه عنصر (primelement) په $\mathbb{Q}$ کي دلاندي خواصو سره:

(i) $P = 3 \nmid a_3 = 1$

(ii) $p = 3 \mid a_2 = 9\ ,\ p = 3 \mid a_1 = 6$

(iii) $p^2 = 9 \nmid a_0 = -3$

څرنګه چه پر f(x) پولینوم باندي د Eisenstein شرطونه صدق کوي ، پس په $\mathbb{Z}$ کي irreducible ده.

تبصره: که د ایزین شتاین (**Eisenstein's criterion**) شرطونه پریوي پولینوم قابل د تطبیق نه وي، بیا هم په عمومي ډول نه شوویلی چه پولینوم reducible (تجزیي وړ) ده. دمثال په ډول:

$f(x) = x^3 + 3x + 18 \in \mathbb{Z}[X]$

د 3 اولیه عدد لپاره (i) او (ii) شرطونه صدق کوي، مګر (iii) صدق نه کوی. ځکه:

$3^2 = 9 \mid a_0 = 18$

مګربیا هم f(x) قابل دتجزیي نه ده.

تعریف 8.9: F یوه ساحه (field) ده او مونږدالاندي پولینوم لرو:

$p(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in F[X]$

د انالیزڅخه پوهیږوچه هره پولینوم په یوه ساحه کي مشتق (differentiable) لري. دا لاندي پولینوم د p(x) د مشتق(differential) په نوم یادیږي:

$p'(x) = n.a_nx^{n-1} + (n-1).a_{n-1}x^{n-2} + ... + 2.a_2x + a_1$

هغه قوانین چه په انالیزکي د مشتق لپاره دي، دلته هم صدق کوي. یعنی د $a \in F$ او $p(x), q(x) \in F[X]$ لیکلی شو:

$(p(x) + q(x))' = p'(x) + q'(x)$, $(a.p(x))' = a. p'(x)$

$(p(x).q(x))' = p'(x).q(x) + p(x). q'(x)$

تعریف 8.10: F یوه ساحه (field) ، L یو توسعه فیلد (extension field) د F او $a \in L$ دی.

$P(x) \in F[X]$

a د p(x) د r مرتبه یي multiple root (مضاعف جذر) په نوم یادیږي، پدي شرط چه :

$(\exists r \in \mathbb{N}, r > 1)$; $p(x) = (x-a)^r . q(x)$, $q(x) \in F[X]$

یا په بل عبارت :

$(x - a)^r \mid p(x) \wedge (x - a)^{r+1} \nmid p(x)$

(یعنی p(x) پر $(x-a)^r$ قابل دتقسیم او پر $(x-a)^{r+1}$ قابل دتقسیم نه وي)

که r = 1 وي، بیا a ته ساده جذروای.

مثال

$p(x) = x^3 - 3x + 2 \in \mathbb{Q}[x]$

$p(x) = x^3 - 3x + 2 = (x - 1)^2 . (x + 2)$

دلته 1 مضاعف جذرچه مرتبه یي 2 او -2 ساده جذردی.

ليما 8.2: F يوه ساحه (field) او L سپليتينګ فيلد (splitting field) د $p(x) \in F[X]$ دی. بيا:

(1) $a \in L$

a يو multiple root (مضاعف جذر)

$$\Leftrightarrow$$

$$p(a) = 0 = p'(a)$$

(2)

p(x) په L کي مضاعف جذر (multiple root) لري

يوه غيرثابته $q(x) \in F[X$ تابع موجوده ده ،چه p(x) او p´(x) پرهغي باندي قابل دتقسيم دي

يعنی:

$$\exists\, q(x) \in F[X]\,, \deg (q(x) > 0\,; q(x) \,|\, p(x) \wedge q(x) \,|\, p'(x)$$

حل (1):

" $\Leftarrow$ " multiple root دتعريف له مخي:

$$(\exists r \in \mathbb{N} \;\wedge\; r > 1)\,; p(x) = (x-a)^r . q(x), \qquad q(x) \in F[X]$$

$$\Rightarrow\; p'(x) = r.\,(x-a)^{r-1}.\; q(x) + (x-a)^r . q'(x)$$

$$\Rightarrow\; p'(a) = r.\,(a-a)^{r-1}.\; q(x) + (a-a)^r . q'(x) = 0+0 = 0$$

" $\Rightarrow$ " ځرنګه چه د L ساحه سپليتينګ (splitting field) ده ، پس د هغه د تعريف له مخی بايد يوه پولينوم p(x) موجوده وي ، چه په خطی فکتورو قابل د تجزيه وي. مونږ فرض کوو ،چه a يي يوجذردی.

که a يو multiple root (مضاعف جذر) د p(x) نه وي ، يعنی:

$$\exists\, q(x) \in F[X]\,, q(a) \neq 0 \;\;\wedge\;\; p(x) = (x-a).\,q(x)$$

$$p'(x) = q(x) + (x-a)q'(x) \;\Rightarrow p'(a) = q(a) + (a-a)q'(a)$$

$$\Rightarrow p'(a) = q(a) \neq 0$$

مګردا خلاف دفرضيي ده. پس بايد a يو multiple root (مضاعف جذر) د p(x) وي

حل (2):

" $\Leftarrow$ " د فرضيي له مخي بايد يو multiple root (جذرمضاعف) $a \in L$ په p(x) کي موجود وي. پدي صورت بيا بايدد (1) له مخي p(a) = 0 = p´(a) صدق وکړي.

مونږ.غواړهغه غيرمستقيم ثبوت کړو. يعني فرض کووچه هغه ډول يوه تابع وجود نه لري. يعنی:

$$\nexists\, q(x) \in F[X]\,, \deg\,(q(x) > 0\,; q(x) \mid p(x) \wedge q(x) \mid p'(x)$$
$$\Rightarrow \gcd(\,p(x), p'(x)\,) = 1$$
$$\Rightarrow \exists\, r(x)\,, s(x) \in F[X]\,,\ \ r(x).\,p(x) + s(x).\,p'(x) = 1$$
$$\Rightarrow r(a).\,p(a) + s(a).\,p'(a) = 1$$
$$\Rightarrow r(a).\,0 + s(a).\,p'(a) = s(a).\,p'(a) = 1$$
$$\Rightarrow p'(a) \neq 0$$

مګردا خلاف دفرضيي ده. پس بايد:

$$\exists\, q(x) \in F[X]\,, \deg\,(q(x) > 0\,; q(x) \mid p(x) \wedge q(x) \mid p'(x)$$

" $\Rightarrow$ " د فرضيي له مخي ليکلی شو:

$$\exists\, q(x) \in F[X]\,, \deg\,(q(x) > 0\,; q(x) \mid p(x) \wedge q(x) \mid p'(x)$$
$$\Rightarrow \exists\, r(x), s(x) \in F[X]\,;\, p(x) = q(x).r(x)\,,\, P'(x) = q(x).s(x)$$

څرنګه چه L يو سپليتينګ فيلد(splitting field) د p(x) او $\deg\,(q(x) > 0$ ده. پس يو $a \in L$ موجود دی ، چه q(a)=0 شی. يعني:

$$p'(a) = q(a).s(a) = 0.s(a) = 0 = p(a)$$

په نتيجه کي p(x) نظر (1) ته په L کي يومضاعف جذرلري.

تبصره: ورپورتني ليما څخه نتيجه اخلو ، چه که p(a)=0 او $p'(a) \neq 0$ باشد ، پدي صورت بيا a د p(x) ساده جذر دی.

مثال 8.12:

$p(x) = x^3 - 2x^2 + x \in \mathbb{Q}[X]$

0 او 1 د p(x) دوه جذرونه دي. 1 مضاعف جذر (multiple root) دی چه مرتبه يی 2 ده. ځکه:

$$p(x) = (x-1)^2\,.\,x$$
$$p'(x) = 3x^2 - 4x + 1$$

پورتنی ليما د (1) له مخي بايد $p(1) = 0 = p'(1)$ او $p(0) = 0 \neq p'(0)$ وي.

$$P(1) = 1^3 - 2.1^2 + 1 = 1 - 2 + 1 = 0$$
$$p'(1) = 3.1^2 - 4.1 + 1 = 3 - 4 + 1 = 0$$

$$p(0) = 0^3 - 2.0^2 + 0 = 0$$
$$p'(0) = 3.0^2 - 4.0 + 1 = 1 \neq 0$$

پورتنی ليما د (2) له مخي بايد:

$$\exists\, q(x) \in F[X]\,, \deg (q(x) > 0\,;\, q(x) \mid p(x) \wedge q(x) \mid p'(x)$$

اوياداچه:

$$\exists\, q(x) \in F[X]\,, \deg (q(x) > 0\,;\, \gcd(p(x), p'(x)) = q(x)$$

مونږ غواړو $\gcd(p(x), p'(x))$ پيداکړو

$$x^3 - 2x^2 + x = \frac{1}{3}x\,.\,(3x^2 - 4x + 1) + -\frac{2}{3}x^2 + \frac{2}{3}x$$

$$3x^2 - 4x + 1 = -\frac{9}{2}\,.\,(-\frac{2}{3}x^2 + \frac{2}{3}x) + (-x + 1)$$

$$-\frac{2}{3}x^2 + \frac{2}{3}x$$

$$= -\frac{2}{3}x\,.\,(-x + 1) + 0$$

پس:

$$\gcd(p(x), p'(x)) = -x + 1 = q(x)$$

مثال 8.13 : مونږد $\mathbb{Z}_5$ فيلد په نظرکي نيسو

$$p(x) = x^3 + \bar{3}x + \bar{4} \in \mathbb{Z}_5\,[x]$$

$$p(\bar{3}) = \bar{3}^3 + \bar{3}.\bar{3} + \bar{4} = (\bar{5}.\bar{5} + \bar{2}) + \bar{3}.\bar{3} + \bar{4}$$

$$= \bar{0} + \bar{2} + \bar{9} + \bar{4}$$

$$= \bar{2} + \bar{4} + \bar{4} = \overline{10} = \bar{2}\,.\,\bar{5} = \bar{2}\,.\,\bar{0} = \bar{0}$$

وليدل شوچه $\bar{3}$ يو جذر د p(x) ده.

$$P'(x) = \bar{3}.x^2 + \bar{3}$$

$$P'(\bar{3}) = \bar{3}.\bar{3}^{\,2} + \bar{3} = \bar{3}\,.\,\bar{9} + \bar{3} = (\bar{5}.\bar{5} + \bar{2}) + \bar{3}$$

$$= \bar{2} + \bar{3} = \bar{0}$$

په نتيجه کي:

$$P(\bar{3}) = \bar{0} = P'(\bar{3})$$

پورتنی ليما له مخي $\bar{3}$ يو multiple root (مضاعف جذر) د p(x) په $\mathbb{Z}_5$ دی.

يعنی:

$$p(x) = x^3 + \bar{3}x + \bar{4} = (x - \bar{3})^2\,.\,(x + \bar{1})$$

نهم فصل

Vieta`s Formulas, Diophantine linaer equation

(ويتا فورمول ، ډيوفينتني خطي معادلي)

تعريف: Vieta`s Formulas (ويتا فورمول)

ويتا (Vieta) يوفرانسوى عالم (1540-1604) وه چه په پولينوم كي دجذرواو ضريبوترمينځ رابطي پيداكړي اود Vieta`s Formulas په نوم ياديږي.

قضيه polynomias und Vieta`s Formulas

كه مونږيوه پولينوم $p(x) \in \mathbb{C}[X]$ په لاندي شكل ولرو :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

د 8.2 قضيي له مخي $p(x)$ پولينوم په خطى فكتوروقابل د تجزيي ده. يعنى $x_1, x_2, \ldots, x_n \in \mathbb{C}$ موجودي چي:

$$p(x) = a_n (x-x_1).(x-x_2)\ldots(x-x_n)$$

دلته $x_1, x_2, \ldots, x_n$ د پولينوم جذرونه دي.

د Vieta فورمول له مخي ديوي پولينومي دجذرو اوضرايبوترمينځ لاندي رابطي موجودي دي:

$$x_1 + x_2 + x_3 + \ldots + x_n = -\frac{a_{n-1}}{a_n}$$

$$x_1 x_2 + x_1 x_3 + \ldots + x_1 x_n + \ldots + x_{n-1} x_n = \frac{a_{n-2}}{a_n}$$

$$x_1 x_2 x_3 + x_1 x_2 x_4 + \ldots + x_{n-2} x_{n-1} x_n = -\frac{a_{n-3}}{a_n}$$

.

.

.

$$x_1 x_2 \ldots x_k + x_1 x_2 \ldots x_{k-1} x_{k+1} + \ldots + x_{n-k+1} x_{n-k+2} \ldots x_n = (-1)^k . \frac{a_k}{a_n}$$

.

.

.

$$x_1 x_2 \ldots x_n = (-1)^n . \frac{a_0}{a_n}$$

البته علامات ورسته دمساوات څخه په منفى (-) شروع كيږى اوپه متناوب ډول مثبت (+) /و منفى (-) كيږي. او اخيرى علامه $(-1)^n$ وي.

مثال8.14 : مونږلاندي $p(x) \in \mathbb{C}[X]$ پولينوم لرو:

$$p(x) = x^2 + x - 6$$

عمومی شکل یي:

$p(x) = a_2x^2 + a_1x + a_0$

په ورتني پولينوم کي :

$n = 2\ , a_2 = 1\ , a_1 = 1\ , a_0 = -6$

(a) جذرونه د Vieta له لياري پيداکوو

که x_1 او x_2 يي جذرونه وي، بيا Vieta د فورمل له مخي ليکلی شو:

$$x_1 + x_2 = -\frac{a_1}{a_2} = -\frac{1}{1} = -1$$

$$x_1 . x_2 = (-1)^2 \frac{a_0}{a_2} = 1.\frac{-6}{1} = -6$$

جذرونو دپيداکولولپاره بايد اعداد پيد اشی چي دپورتنيي معادلي صدق وکړی. هغه اعداد $x_1=2$ او $x_2=-3$ دي. ځکه:

$$x_1 + x_2 = 2 - 3 = -1$$

$$x_1 . x_2 = 2. (-3) = -6$$

امتحان:

$$p(2) = 2^2 + 2 - 6 = 6 - 6 = 0$$

$$p(-3) = (-3)^2 + (-3) - 6 = 9 - 9 = 0$$

له دي څخه نتيجه اخلوچه د نوروطريقو ترڅنګ ديوي دويمي درجي پولينومي جذرد Vieta فورمل له مخه هم پيدا کولای شو

(b) دويمه درجه پولينوم پيداکوو چي $(x_1)^2$ او $(x_2)^2$ يي جذرونه وي. مونږهغه پولينوم په g(x) ښيوو. البته دلته x_1 او x_2 دپورتنی p(x) پولينوم جذرونه دي

$g(x) = x^2 + b_1x + b_0$

په (a) کي موولیدل چي:

$$x_1 + x_2 = -1$$

$$x_1 . x_2 = -6$$

$$(x_1)^2 + (x_2)^2 = (x_1 + x_2)^2 - 2.\ x_1.\ x_2$$

$$= (-1)^2 - 2.(-6) = 1+12 = 13 = -\frac{b_1}{1} = -b_1$$

$$(x_1)^2 . (x_2)^2 = (x_1.\ x_2)^2 = (-6)^2 = 36 = \frac{b_0}{1} = b_0$$

$$b_1 = -13\ , b_0 = 36$$

په نتيجه کي g(x) لاندي شکل لري:

$$g(x) = x^2 + b_1x + b_0 = x^2 - 13x + 36$$

امتحان:

$$(x_1)^2 = (2)^2 = 4\ , \ (x_2)^2 = (-3)^2 = 9$$

$$g(4) = 4^2 - 13.4 + 36 = 16 - 52 + 36 = 0$$

$$g(9) = (9)^2 - 13.9 + 36 = 81 - 117 + 36 = 0$$

ومولیدل چه 4 او9 د $g(x)$ دي
مثال : مونږدالاندي د $p(x) \in \mathbb{C}[X]$ پولينوم لرو:

$$p(x) = 3x^2 - 2x - 1$$

عمومی شکل يي:

$$p(x) = a_2x^2 + a_1x + a_0$$

مونږپه $p(x)$ کي لرو:

$$n = 2 \ , a_2 = 3 \ , a_1 = -2 \ , a_0 = -1$$

که x_1 او x_2 يي جذرونه (حل) وي، بيا Vieta د فورمل له مخي ليکلی شو:

$$x_1 + x_2 = -\frac{a_1}{a_2} = -\frac{-2}{3} = \frac{2}{3} \qquad (I)$$

$$x_1 \cdot x_2 = (-1)^2 \frac{a_0}{a_2} = -\frac{1}{3}$$

$x_1 = 1$ يو جذردهغي معادلي دی.ځکه:

$$p(1) = 3.1^2 - 2.1 - 1 = 0$$

اوس (I) معادله څخه دويم جذرپيداکوو

$$x_1 + x_2 = \frac{2}{3} \implies x_2 = \frac{2}{3} - x_1 = \frac{2}{3} - 1 = -\frac{1}{3}$$

امتحان:

$$p\left(\frac{-1}{3}\right) = 3.\left(\frac{-1}{3}\right)^2 - 2.\left(\frac{-1}{3}\right) - 1 = \frac{1}{3} + \frac{2}{3} - 1 = 0$$

مثال : مونږلاندي $p(x) \in \mathbb{C}[X]$ پولينوم لرو:

$$p(x) = x^4 - 5x^3 + 5x^2 + 5x - 6$$

عمومی شکل يي:

$$p(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

دلته:

$$n = 4 \ , a_4 = 1 \ , a_3 = -5 \ , a_2 = 5 \ , a_1 = -5 \ , a_0 = -6$$

که x_1 ، x_2 ، x_3 او x_4 يي جذرونه وي، بيا Vieta د فورمل له مخي:

$$x_1 + x_2 + x_3 + x_4 = -\frac{a_3}{a_4} = -\frac{-5}{1} = 5$$

$$x_1 . x_2 + x_1 . x_3 + x_1 . x_4 + x_2 . x_3 + x_2 . x_4 + x_3 . x_4 = \frac{a_2}{a_4} = \frac{5}{1} = 5$$

$$x_1 . x_2 . x_3 + x_1 . x_2 . x_4 + x_2 . x_3 . x_4 = -\frac{a_1}{a_4} = -\frac{5}{1} = -5$$

$x_1 . x_2 . x_3 . x_4 = (-1)^4.\frac{a_0}{a_4} = 1.\frac{-6}{1} = -6$

که 2,-1,1 يي جذرونه وي.بيا غواړوپنځم جذريي پيدا کړو

$x_1 + x_2 + x_3 + x_4 = 1 - 1 + 2 + x_4 = 5 \Longrightarrow x_4 = 5 - 2 = 3$

امتحان:

$p(1) = p(-1) = p(2) = p(3) = 0$

مثال : مونږ لاندي $p(x) \in \mathbb{C}[X]$ پولينوم لرو:

$p(x) = 2x^3 - x^2 + 2x - 1$

عمومی شکل يي:

$p(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$

دلته:

$n = 3 \ , a_3 = 2 \ , a_2 = -1 \ , a_1 = 2 \ \ , a_0 = -1$

که x_1 ، x_2 او x_3 يي جذرونه وي، بيا Vieta د فورمل له مخي:

$x_1 + x_2 + x_3 = -\ \frac{a_2}{a_3} = -\ \frac{-1}{2} = \frac{1}{2}$

$x_1 . x_2 + x_1 . x_3 + x_2 . x_3 = \frac{a_1}{a_3} = \frac{2}{2} = 1$

$x_1 . x_2 . x_3 = (-1)^3.\frac{a_0}{a_3} = -1.\frac{-1}{2} = \frac{1}{2}$

که i او i- يي وي. غواړودريم جذرپيداکړو

$x_1 + x_2 + x_3 = i - i + x_3 = \frac{1}{2} \quad \Longrightarrow x_3 = \frac{1}{2}$

مثال : مونږ لاندي $p(x) \in \mathbb{C}[X]$ پولينوم لرو:

$p(x) = x^3 - 2x^2 + x - 2$

$p(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$

دلته:

$n = 3 \ , a_3 = 1 \ , a_2 = -2 \ , a_1 = 1 \ \ , a_0 = -2$

که x_1 ، x_2 او x_3 يي جذرونه وي، بيا Vieta د فورمل له مخي:

$x_1 + x_2 + x_3 = -\ \frac{a_2}{a_3} = -\ \frac{-2}{1} = 2$

$x_1 . x_2 + x_1 . x_3 + x_2 . x_3 = \frac{a_1}{a_3} = \frac{1}{1} = 1$

$x_1 . x_2 . x_3 = (-1)^3.\frac{a_0}{a_3} = -1.\frac{-2}{1} = 2$

ليدل کيږی چی i او 2 يي جذرونه دي. غواړو دريم جذريي پيداکوو

$x_1 + x_2 + x_3 = i + 2 + x_3 = 2 \quad \Longrightarrow x_3 = 2 - 2 - i = -i$

تمرين : مونږ لاندي $p(x) \in \mathbb{C}[X]$ پولينوم لرو:

$p(x) = 2x^4 - x^3 + 5x^2 - 6x + 2$

که دري جذرونه يي لاندي اعداد وی:

$x_1 = 1$, $x_2 = i\sqrt{2}$, $x_3 = -i\sqrt{2}$

څلورم جذريي څودی

تعریف:Diophantine linear equation (ديوفنتينی خطی معادلي)

دا لاندي خطی معادله ديو يونانی عالم Diophantine په نوم ياديږي:

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c \qquad (c, a_i \in \mathbb{Z}, i = 1,2,\dots,n)$$

ديوفنتينی (Diophantine) پيداکړچه څه وخت دپورتني معادلي حل تام اعداد وي. مګرمونږدلته فقط دوه مجهوله خطی معادلي مطالعه کوو

$$a.x + b.y = c \qquad (a, b, c \in \mathbb{Z})$$

ديوفنتينی (Diophantine) پيدا کړچه پورتنی معادله هغه وخت دتام اعدادو حل لري، پدي شرط چه c پر $\gcd(a, b)$ باندي قابل دتقسيم وي. البته داډول معادلي څوحله لري. مونږفرض کووچه $\gcd(a, b) = g$ دی. د حل لپاره يي مونږ ددو لاندي طريقوڅخه استفاده کوو:

لمړی: **د Euclidean Algorithm طريقه:** د Euclidean Algorithm له مخي کولای شو r او s اعداد دلاندي خواص سره پيدا کړو:

$$g = \gcd(a, b) = a.r + b.s$$

که $d := c/g$ وي،بيا:

$$g.d = a.(d.r) + b.(d.s)$$
$$c = a.(d.r) + b.(d.s)$$

د معادلي يوحل :

$$x_0 := d.r \ , y_0 := d.s$$

د معادلي هوموګين (homogene) حل په لاندي ډول پيدا کولای شو:

$$\gcd(a, b) = g \implies \exists\, a_1, a_1 \in \mathbb{Z} \,;\, a = g.a_1 \ , b = g.b_1$$

$$ax + by = 0$$
$$g.a_1.x + g.b_1.y = 0 \implies a_1.x = -b_1.y$$

پورتني معادله دالاندي پاراميتري حل لري:

$$x_1 = b_1t\,,\ y_1 = -a_1t \qquad (t \in \mathbb{Z})$$

ځکه:

$$a_1.x_1 = a_1.b_1.t \ , -b_1.y_1 = -b_1.(-a_1).t = b_1.a_1.t$$
$$\implies a_1.x_1 = -b_1.y_1$$

عمومی حل يي:

$$(x,y) = (x_1,y_1) + (x_0,y_0) = (b_1t, -a_1t) + (x_0,y_0)$$

$$= \{(b_1t + x_0\ , -(a_1t + y_0)\ )\quad (\ t \in \mathbb{Z}\ )\}$$

دويم: Fermat-Euler له لياري:

$$\gcd(a,b) = 1 \quad \Longrightarrow\ a^{\varphi(b)} \equiv 1 (\mathrm{mod}\ b)$$

$\varphi(b)$ اويلرفنكشن (Euler-Function) ده چه په تيروفصلومطالعه شوى اوپه لاندي شكل ده:

$$\varphi(b) = \ |\{k \in \mathbb{N}\ |\ 1 \le k \le b\ \wedge\ gcd(b,k) = 1\}|$$

د $a.x\ + b.y = c$ معادله د Fermat-Euler **له لياري** لاندي حل لري:

$$x \equiv c.a^{\varphi(b)-1}\ \ (\mathrm{mod}\ b)$$

يعنى:

$$x = c.a^{\varphi(b)-1} + tb \quad (\ t \in \mathbb{Z}\ )$$

$$y = c.\frac{1 - a^{\varphi(b)}}{b} - ta \quad (\ t \in \mathbb{Z}\ )$$

مثال:

$$6x + 10y = 100$$

دلته: $a = 6\ , b = 10\ , c = 100$

$$10 = 1.6 + 4$$
$$6 = 1.4 + 2$$
$$4 = 2.2 + 0$$

پس:

$$\gcd\ (10{,}6) = 2$$

$$\frac{c}{\gcd(a,b)} = \frac{100}{2} = 50$$

څرنګه چه د ديوفنتينى (Diophantine) شرط صدق كوي، پس معادله دتامو اعدادو حل لري .

حل د Euclidean Algorithm له لياري:

د حل لپاره بايد r او s اعداد پيداكړو چه دالاندي معادله صدق كړي:

$$\gcd(a,b) = a.r + b.s$$

$2 = 6 - 1.4 = 6 - 1(10 - 1.6) = 2.6 - 1.10$

پیدا موکړچه $r = 2 , s = -1$ او یو حل يي:

$x_0 = r.d = 2.50 = 100 , \qquad y_0 := s.d = -1.50 = -50$

اوس د هغي معادلي هوموګین (homogene) حل پیدا کوو

$6x + 10y = 0$

$2.3.x + 2.5.y = 0 \implies 3.x + 5.y = 0 \implies 3.x = -5.y$

پورتني معادله فوق لاندي حل لري:

$x_1 = 5t , \ y_1 = -3t \qquad (t \in \mathbb{Z})$

عمومی حل یی:

$$(x, y) = (x_1, y_1) + (x_0, y_0) = (5t, -3t) + (100, -50)$$

$$= \{(5t + 100, -(3t + 50)) \ (t \in \mathbb{Z})\}$$

پس دحل سیت يي:

$$\{(x, y) | \ x = 100 + 5t, y = -50 - 3.t \ (t \in \mathbb{Z}) \}$$

امتحان: که $t = 2$ وي:

$(x, y) = (5t + 100, -(3t + 50) = (2.5 + 100, -(2.3 + 50))$

$= (110, -56)$

اوس $(x, y) = (110, -56)$ په راکړل شوي معادله کي وضع کوو

$6.110 + 10.(-56) = 660 - 560 = 100$

پس $(x, y) = (110, -56)$ د معادلي یو حل اوتام اعداد دي.

حل د Fermat-Euler له لاري:

$6x + 10y = 100 , \gcd(6,10) = 2$

$$\frac{6}{2}x + \frac{10}{2}y = \frac{100}{2} \implies \quad 3x + 5y = 50$$

په پورتني معادله کي $a = 3 , b = 5 , c = 50$

څرنګه چه $\gcd(3,5) = 1$ دی، پس د Fermat-Euler طریقه قابل د تطبیق ده

$\varphi(b) = \varphi(5) = |\{k \in \mathbb{N} \ | \ 1 \leq k \leq 5 \ \wedge \ gcd(5, k) = 1\}| = 4$

$$x = c.a^{\varphi(b)-1} + tb \quad (t \in \mathbb{Z})$$

$$= 50.3^{4-1} + 5t \quad (t \in \mathbb{Z}) = 50.3^{4-1} + 5t \quad (t \in \mathbb{Z})$$

$$= 50.3^3 + 5t \quad (t \in \mathbb{Z}) = 1350 + 5t \quad (t \in \mathbb{Z})$$

$$y = c.\frac{1 - a^{\varphi(b)}}{b} - ta \quad (t \in \mathbb{Z}) = 50.\frac{1 - 3^4}{5} - 3.t \quad (t \in \mathbb{Z})$$

$$= 50.\frac{-80}{5} - 3.t \quad (t \in \mathbb{Z}) = -800 - 3.t \quad (t \in \mathbb{Z})$$

پس دحل سیت یي:

$$\{(x, y) | \ x = 1350 + 5t, y = -800 - 3.t \quad (t \in \mathbb{Z}) \ \}$$

امتحان: که $t = 0$ وي

$(x, y) = (1350, -800)$

$6x + 10y = 100$

اوس $(x, y) = (1350, -800)$ په پورتني معادله کي وضع کوو

$6.1350 + 10.(-800) = 8100 - 8000 = 100$

پس $(x, y) = (1350, -800)$ د معادلي یو حل اوتام اعداد دي.

مثال:

$168x + 238y = 126$

دلته $a = 168 \, , b = 238 \, , c = 126$

$238 = 1.168 + 70$

$168 = 2.70 + 28$

$70 = 2.28 + 14$

$28 = 2.14 + 0$

پس:

$\gcd (238,168) = 14$

$$\frac{c}{\gcd(a, b)} = \frac{126}{14} = 9$$

څرنګه چه د دیوفنتینی (Diophantine) شرط صدق کوي، پس معادله دتامو اعدادو حل لري .

حل د Euclidean Algorithm له لیاري:

د حل لپاره باید r او s اعداد پیداکړو چه دالاندي معادله صدق کړي:

$\gcd(a, b) = a.r + b.s$

$14 = 70 - 2.28$

$\quad = 70 - 2(168 - 2.70)$

$\quad = 238 - 168 - 2(168 - 2(238 - 168))$

$$= 238 - 168 - 2(168 - 2.238 + 2.168)$$
$$= 238 - 168 - 2.168 + 4.238 - 4.168$$
$$= 5.238 - 7.168$$

پيداموکړچه $r = -7 , s = 5$ اويو حل يي:

$$x_0 = r.d = -7.9 = -63 , \qquad y_0 := s.d = 5.9 = 45$$

اوس د هغي معادلي هوموګين (homogene) حل پيدا کوو

$$168x + 238y = 0$$
$$14.12.x + 14.17.y = 0 \implies 12x + 17.y = 0$$
$$\implies 12x = -17.y$$

پورتني معادله لاندي حل لري:

$$x_1 = 17t , \; y_1 = -12t \qquad (t \in \mathbb{Z})$$

عمومی حل يي:

$$(x,y) = (x_1,y_1) + (x_0,y_0) = (17t,-12t) + (-63,45)$$
$$= (17t - 63, -12t + 45) \quad (t \in \mathbb{Z})$$

پس دحل سيت يي:

$$\{(x,y)|\, x = -63 + 17t, y = 45 - 12.t \quad (t \in \mathbb{Z}) \}$$

تمرين: مونږ لاندي معادله لرو:

$$4x + 6y = 16$$

(a) ثبوت کړی چه د ديوفنتينی (Diophantine) شرط په پورتني معادله کي صدق کوي

(b) معادله د Euclidean Algorithm او Fermat-Euler له لياري حل کړی

تمرين: احمد غواړي يوکتاب په 23 افغانی راونيسي. احمد يوازي 2 افغانيګي له ځان سره لري او دکاندارفقط 5 افغانيګی پيسي په دکان کي لري. معلوم کړي چه احمد د کتاب رانيولولپاره بايد څو دوه افغانيګی دکاندارته او دکاندار څو 5 فغانيګی احمد ته ورکړي

(a) عمومی حل يي د ديوفنتينی (Diophantine) معادلياري پيداکړي

(b) د عمومی حل له مخي پيدا کړي چه 14 دوه افغانيګی او يو 5 افغانيګی هم حل دی

لسم فصل

Cryptography(رمز لیکنه)

د کراپیتوگرافی بواسطه کولای شودیوپیغام متن په یورمزي پیغام (encryption message) تبدیل کړوچي هرڅوک هغه ونشي لوستلی . فقط یوازي هغه کسان چه اجازه دلوستلوولري ، کولاي شي پیغام بیرته په اصلی شکل (decryption message) راولي. په اوسني Cryptography (رمزلیکنه) کي دمعاصرالجبردفکتوري گروپو (factor groups) څخه زیاته استفاده کیږي.
ددي کارلپاره دنوروترڅنګ د ASCII-Code (اویا ISO-Code) استعمالوي.
په ASCII-Code کي دحرفونو اواعدادو ترمینځ رابطه موجوده ده . یعني په جدول کي دهرحرف لپاره یوعدد تعین شویدی (همدارنگه دسمبولولپاره).
کمپیوتري پروگرامونه موجود دي، چي د هغوي پواسطه په ASCII جدول کي د حرف (یا سیمبول) مربوطه عدد اوعدد ته ترتیب شوی حرف (یا سمبول) په اسانه پیداکولی شي. پیغام استونکی (sender) او پیغام اخیستونکی (receiver) یو بل سره د یوډول جدل داستعمال لپاره موافقه کوي. مګرمونږ دلته دمثالولپاره خپل لاندي جدول استعمالو:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z	?	=	%	#
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

مونږ دحرف (یا سیمبول) اوعدد ترمینځ رابطه په " $\sim$ " سره ښیو
د رمزلیکني لپاره مختلفي طریقي لکه Polig-Hellan, ElGamal او RSA-Method موجود دي.
پیغام استوونکی (Sender) په S او پیغام اخیستوونکی (Receiver) په R ښیو.

Pohlig-Hellman Cryptsystem (1)

پدي سیستم کي پیغام استوونکی(S) او پیغام اخیستوونکی(R) پریولوي اولیه عدد p (prime number) موافقه کوي

د S وظیفه:

(a) یو عدد e د لاندي خواصوسره انتخابوي او R ته خبرورکوي:

$e \in \{2, \ldots, p-2\} \quad \wedge \; gcd(e, p-1) = 1$

(b) په جدول کي د پیغام د متن لپاره مربوطه اعداد پیدا کوي اوبیا هغه د $(\mathbb{Z}^*_p, .)$ عنصرپه شکل لیکي. یعني که m دیوحرف مربوطه عدد وي، بیا هغه د

په شکل ليکي $\overline{m} \in (\mathbb{Z}^*{}_p,.)$

(c) اصلي پيغام په رمزي پيغام (encryption message) په لاندي ډول بدلوي:

$$\bar{c} := (\overline{m})^e$$

(d) رمزي پيغام $\bar{c}$ پيغام اخيستونکي ته ليږي

د R وظيفه:

(a) يو عدد d دلاندي خواصوسره انتخابوي:

$$d \in \{2, \dots, p-2\} \quad \wedge \quad \text{e.d} \equiv 1 \ (\text{mod p} - 1)$$

(b) رمزي پيغام $\bar{c}$ بيرته په اصلي پيغام (decryption message) په لاندي ډول بدلوي:

$$\overline{m} = (\bar{c})^d$$

مثال : S غواړي يو پيغام دمثال په ډول د AFG پيغام اخيستونکي ته ليږي.
دواړه پريو اوليه اعداد $p = 11$ موافقه کوي. دي کارلپاره د $(\mathbb{Z}^*{}_{11},.)$ گروپ ځخه استفاده کوي.

د S وظيفه:

(a) يو عدد e د لاندي خواصوسره انتخابوي او R ته خبرورکوي:

$$e = 3 \in \{2, \dots, p-2\} \ \wedge \quad gcd(3,10) = 1$$

(b) د جدول له مخي د پيغام مربوطه اعداد دادي:

$$A \rightsquigarrow 1 \ , \text{F} \rightsquigarrow 6 \ , \text{G} \rightsquigarrow 7$$

اوهغه په عددي رمزی پيغام په لاندي ډول تبديلوي:

$$\text{m} := 1 \ , \ \overline{\text{m}} := \bar{1} \in (\mathbb{Z}^*{}_{11},.) \ , \bar{c} = (\overline{m})^e = (\bar{1})^3 = \bar{1}$$

$$\text{m} := 6 \ , \ \overline{\text{m}} := \bar{6} \in (\mathbb{Z}^*{}_{11},.)$$

$$\bar{c} = (\overline{m})^e = (\bar{6})^3 = \overline{36}.\bar{6} = \bar{3}.\bar{6} = \bar{7}$$

$$\text{m} := 7 \ , \ \overline{\text{m}} := \bar{7} \in (\mathbb{Z}^*{}_{11},.)$$

$$\bar{c} = (\overline{m})^e = (\bar{7})^3 = \overline{49}.\bar{7} = \bar{5}.\bar{7} = \bar{2}$$

$$\text{E} := \{\bar{1}, \bar{7}, \bar{2}\}$$

(c) رمزی عددي پيغام $E := \{\bar{1}, \bar{7}, \bar{2}\}$ پيغام اخيستونکي R ته ليږي

د R وظيفه:

(a) يو عدد d د لاندي خواصوسره انتخابوي:

$$d = 7 \in \{2, \dots, p-2\} \quad \wedge \quad \text{e.d} = 3.7 = 21 \equiv 1 \ (\text{mod } 10)$$

(b) رمزی عددی پيغام $\text{E} := \{\bar{1}, \bar{7}, \bar{2}\}$ اخلي. مربوطه حروف يي:

$$1 \rightsquigarrow \text{A} \ , 7 \rightsquigarrow \text{G} \ , 2 \rightsquigarrow \text{B}$$

يعني رااليږل شوي پيغام AGB دی

(c) بیا دا رمزی عددي پیغام په اصلي عددي پیغام په لاندي ډول بدلوي:
$\bar{c} := \bar{1}$, $\bar{m} = (\bar{c})^d = (\bar{1})^7 = \bar{1}$.
$\bar{c} := \bar{7}$
$\bar{m} = (\bar{c})^d = (\bar{7})^7 = (\bar{7})^2 . (\bar{7})^2 . (\bar{7})^2 . \bar{7} = \bar{5} . \bar{5} . \bar{5} . \bar{7} = \overline{25} . \overline{35}$
$= \bar{3} . \bar{2} = \bar{6}$
$\bar{c} := \bar{2}$
$\bar{m} = (\bar{c})^d = (\bar{2})^7 = (\bar{2})^4 . (\bar{2})^3 = \overline{16} . \bar{8} = \bar{5} . \bar{8} = \overline{40} = \bar{7}$

عددي اصلي پیغام $D := \{\bar{1}, \bar{6}, \bar{7}\}$ دی
جدول له مخي :

$$1 \leadsto A \ , 6 \leadsto F \ , 7 \leadsto G$$

معلوم شوچه اصلي پیغام AFG دی

(2) RSA-Cryptsystem

د RSA رمزلیکني طریقه ددری ریاضي عالمانو Shamir, Adleman او Rivest په 1978 کال کي کشف شوه. د RSA طرزالعمل په لاندي ډول دي:

(1) public key: پیغام استوونکی (sender) اوپیغام اخیستونکي (receiver) په خپل مینځ کي په یوي public key (عمومي کیلي) سره تفاهم کوي.

(2) private key : دا کیلي فقط یوازي پیغام اخیستونکي ته معلومه ده مونږ پیغام استوونکی کس په S اوپیغام اخیستونکي په R سره ښیو.

د RSA طرزالعمل لاندي مرحلي لري:

د R (وظیفه):

R (i) دوه لوي مختلف اولیه اعداد (prime number) p ، q اینتخابوي اوبیا $n := p.q$ وضع کوي

(ii) د Euler-Function له مخي د $\varphi(n)$ قیمت پیدا کوي. یعنی:

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \mapsto \varphi(n) = |\{k \in \mathbb{N} \mid 1 \leq k \leq n \ \wedge \ gcd(n,k) = 1\}|$$

یا

$$\varphi(n) = (p-1).(q-1)$$

ځکه p او q اولیه اعداد دي

(iii) یوطبیعی عدد e د لاندي خواصوسره انتخابوي اوبیا یي د $\mathbb{Z}_{\varphi(n)}$ عنصرپه شکل لیکي

$$e \in \{2, \dots, \varphi(n)\} \quad \wedge \ gcd\big(e, \varphi(n)\big) = 1$$
$$\bar{e} \in \mathbb{Z}_{\varphi(n)}$$

(iv) یو طبیعی عدد d لاندي خواصوسره پیدا کوي:

$d \in \mathbb{N} \quad \wedge \; \mathrm{d.e} \; \equiv \; 1\big(\mathrm{mod}\, \varphi(n)\big)$

یعنی $\bar{d}$ معکوس د $\bar{e}$ په $\mathbb{Z}_{\varphi(n)}$ رینګ کي دی

دلته (e, n) عمومی کیلی (public key) او (d, n) خصوصی کیلي

(private key) د R (پیغام اخیستونکي) دي. یوازي R هغه پیژني

پیغام استوونکی(S) وظیفه :

(i) عمومی کیلي (e, n) د R څخه لاسته راوړي

(**ii**) په جدول کي د پیغام د متن لپاره مربوطه اعداد پیدا کوي اوبیا هغه د $\mathbb{Z}_n$ عنصرپه شکل لیکي. یعني که m دیوحرف مربوطه عدد وي، بیا هغه $\bar{m} \in \mathbb{Z}_n$ انتخابوي

(iii) د e او $\bar{m}$ په کومک $\bar{c}$ رمزی پیغام په $\mathbb{Z}_n$ کي په لاندي ډول لاسته راوړي:

$\bar{c} \coloneqq (\bar{m}\,)^{\mathrm{e}}$

(iv) $\bar{c}$ عددي رمزی پیغام R (پیغام اخستونکي) ته هستوي

اوس R هغه $\bar{c}$ رمزی پیغام په $\bar{m}$ اصلی پیغام په لاندي ډول بدلوي:

$(\bar{c}\,)^{\,\mathrm{d}} = (\bar{m}\,)^{\mathrm{ed}} = \bar{m}$

مثال: فاطمه غواړي یوپیغام دمثال په ډول '4' مینا ته ولیږي

(a) فاطمه باید لاندي عملیات ترسره کړي :

(1) دوه لمړني اعداد (prime number) p او *q* انتخابوي اوبیادهغوي څخه n لاسته راوړي.یعني:

$\mathrm{p} = 3\,, \mathrm{q} = 11\,, \mathrm{n} = \mathrm{p.q} = 3.11 = 33$

$\varphi(33) = |\{k \in \mathbb{N} \mid \; 1 \leq k \leq 33 \;\wedge\; gcd(33, k) = 1\}| = 20$

یا:

$\varphi(n) = (\mathrm{p} - 1).(\mathrm{q} - 1)$

$\varphi(33) = (3 - 1).(11 - 1) = 20$

ځکه p او *q* اولیه اعداد دي

(2) د e طبعی عدد دلاندي خواصوسره انتخاب شي :

$e \in \{2, \dots, \varphi(n) - 1\} \quad \wedge \; gcd\big(e, \varphi(n)\big) = 1$

$e{:} = 7$

$e = 7 \; \in \{2, \dots, 19\} \;\wedge\; \mathrm{gcd}(7,20) = 1$

$\bar{7} \in \mathbb{Z}_{20}$

(3) یو طبعی عدد d دلاندي خواصوسره پیداکوي:

$d \in \mathbb{N} \quad \wedge \ \mathrm{d.e} \ \equiv \ 1\big(\mathrm{mod}\ \varphi(n)\big)$

یعنی $\bar{d}$ باید معکوس د $\bar{e}$ په $\mathbb{Z}_{20}$ رینګ کي وي
د euclidean algorithm له مخي تام اعداد d او k دلاندي خواصوسره موجود دي:

$\mathrm{d.e} + \mathrm{k}.\varphi(n) = 1 = gcd\big(e, \varphi(n)\big)$
$\mathrm{d}.7 + \mathrm{k}.20 = 1 = gcd(7,20)$

$20 = 2.7 + 6$
$7 = 1.6 + 1$
$6 = 6.1 + 0$

$1 = 7 - 1.6$
$\quad = 7 - 1.(20 - 2.7)$
$\quad = 3.7 - 1.20$
$\quad = 3.7 - 1.20 \Longrightarrow \ \bar{1} = \bar{3}.\bar{7} - \bar{1}.\overline{20} = \bar{3}.\bar{7} - \bar{1}.\bar{0} = \bar{3}.\bar{7}$

په نتیجه کي $\bar{3}$ معکوس د $\bar{7}$ په $\mathbb{Z}_{20}$ رینګ او $d = 3$ دی.
(4) لاندي عمومي او خصوصي کیلي ترتیبوي:
$\text{public key:} \quad (\mathrm{e,n}) = (7{,}33) \ \wedge \ \text{ private key:} \ (\mathrm{d,n}) = (3{,}33)$
(5) فاطمه استونکي پیغام '4' د $\mathbb{Z}_{33}$ دعنصرپه شکل لیکي اوبیاي په رمزی پیغام بدلوي
$\bar{m} := \bar{4} \in \mathbb{Z}_{33}$
$\bar{c} = (\bar{m})^e = (\bar{4})^7 = (\bar{4})^4.(\bar{4})^3 = \overline{256}.\overline{64}$
$\quad = (7.\overline{33} + \overline{25}).(\overline{33} + \overline{31})$
$\quad = (\bar{0} + \overline{25}).(\bar{0} + \overline{31}) = \overline{775} = 23.\overline{33} + \overline{16} = \overline{16}$
رمزی پیغام $\bar{c} = \overline{16}$ دی
(6) رمزي پیغام $\bar{c} = \overline{16}$ مینا ته لیږي
(b) مینا باید لاندي عملیات اجراکړي:
(1) دفاطمي څخه د عمومی کیلي (public key) اورمزي پیغام اخلي. یعني:
$\bar{c} = \overline{16} \in \mathbb{Z}_{33} \quad , \text{ public key:} \quad (\mathrm{e,n}) = (7{,}33)$
(2) مینا بیا هغه رمزی بیغام په په اصلي بدلوي:
$(\bar{c})^d = (\overline{16})^3 = \overline{4096} = \overline{124}.\overline{33} + \bar{4} = \bar{4}$
په نتیجه کي معلوم شوچه اصلی پیغام 4 وه
مثال: پدي مثال کي احمد غواړي یوپیغام د "BALKH" په نامه قادر ته ولیږي.
قادردلتهp او q دپورتني مثال انتخاب کوي.

$p = 3, q = 11, n := p.q = 3.11 = 33$

public key: $(e,n) = (7,33) \wedge$ private key: $(d,n) = (3,33)$

د جدول له مخي:

$B \rightsquigarrow 2, A \rightsquigarrow 1, L \rightsquigarrow 12, K \rightsquigarrow 11, H \rightsquigarrow 8$

احمد اصلی پیغام په لاندي ډول په عددي رمزی(encryption) پیغام بدلوي:

$\bar{m}_1 = \bar{2} \in \mathbb{Z}_{33}, \bar{m}_2 = \bar{1} \in \mathbb{Z}_{33}, \bar{m}_3 = \overline{12} \in \mathbb{Z}_{33}$

$\bar{m}_4 = \overline{11} \in \mathbb{Z}_{33}, \bar{m}_5 = \bar{8} \in \mathbb{Z}_{33}$

$(\bar{m}_1)^e = (\bar{2})^7 = \overline{128} = \bar{3}.\overline{33} + \overline{29} = \overline{29} = \overline{c_1}$

$(\bar{m}_2)^e = (\bar{1})^7 = \bar{1} = \overline{c_2}$

$(\overline{m_3})^e = (\overline{12})^7 = (\overline{12})^3.(\overline{12})^3.\overline{12} = \overline{1728}.\overline{1728}.\overline{12}$

$= (\overline{52}.\overline{33} + \overline{12}).(\overline{52}.\overline{33} + \overline{12})\,\overline{12}$

$= (\bar{0} + \overline{12}).(\bar{0} + \overline{12}).\overline{12}$

$= \overline{1728} = \overline{52}.\overline{33} + \overline{12} = \overline{12} = \overline{c_3}$

$(\bar{m}_4)^e = (\overline{11})^7 = (\overline{11})^3.(\overline{11})^3.\overline{11} = \overline{1331}.\overline{1331}.\overline{11}$

$= (\overline{40}.\overline{33} + \overline{11}).(\overline{40}.\overline{33} + \overline{11})\,\overline{11}$

$= (\bar{0} + \overline{11}).(\bar{0} + \overline{11}).\overline{11}$

$= \overline{11331} = \overline{40}.\overline{33} + \overline{11} = \overline{11} = \overline{c_4}$

$(\overline{m_5})^e = (\bar{8})^7 = (\bar{8})^3.(\bar{8})^3.\bar{8} = \overline{512}.\overline{512}.\bar{8}$

$= (\overline{15}.\overline{33} + \overline{17}).(\overline{135}.\overline{33} + \overline{17}).\bar{8}$

$= (\bar{0} + \overline{17}).(\bar{0} + \overline{17}).\bar{8}$

$= \overline{2312} = \overline{70}.\overline{33} + \bar{2} = \bar{2} = \overline{c_5}$

احمد لاندي عددي رمز محمود ته لیږي:

$E := \{\overline{c_1}\ , \overline{c_2}, \overline{c_3}, \overline{c_4}\ , \overline{c_5}\} = \{\overline{29}\ , \overline{1}, \overline{12}\ , \overline{11}\ , \overline{2}\}$

قادر رمزی عددی پیغام $E := \{\overline{29}\ , \overline{1}, \overline{12}\ , \overline{11}\ , \overline{2}\}$ اخلي. مربوطه حروف يي:

$29 \rightsquigarrow \%\ \ , 1 \rightsquigarrow A\ \ , 12 \rightsquigarrow L, 11 \rightsquigarrow K, 2 \rightsquigarrow B$

یعني رالیږل شوي رمزي پیغام ALKB% دی

قادر هغه رمزی عددی پیغام $E = \{\overline{29}\ , \overline{1}, \overline{12}\ , \overline{11}\ , \overline{2}\}$ اخلي اوپه اصلی پیغام (decryption) يي په لاندي ډول بدلوي :

$$(\ \overline{c_1}\ )^d = ((\ \overline{m_1}\ )^e)^d = ((\overline{2})^7)^3 = (\ \overline{29}\ )^3$$
$$= \overline{24389} = 739.\ \overline{33} + \overline{2} = \overline{2} = \overline{m_1}$$
$$(\ \overline{c_2}\ )^d = (\overline{1})^3 = \overline{1} = \overline{m_2}$$
$$(\ \overline{c_3}\ )^d = (\overline{12})^3 = \overline{12} = \overline{m_3}$$
$$(\ \overline{c_4}\ )^d = (\overline{11})^3 = \overline{11} = \overline{m_4}$$
$$(\ \overline{c_5}\ )^d = (\overline{2})^3 = \overline{8} = \overline{m_5}$$

$$m_1 = 2\ , m_2 = 1\ , m_3 = 12\ , m_4 = 11\ , m_5 = 8$$

اوس قادرپورتني اعداد د جدول له مخي په صلی پیغام بدلوي. یعنی:

$2 \rightsquigarrow B\ , 1 \rightsquigarrow A\ , 12 \rightsquigarrow L, 11 \rightsquigarrow K\ , 8 \rightsquigarrow H$

په نتیجه کي قادرپوهیږي چه لیږل شوي پیغام "*BALKH*„ وه.

Elgamal-Cryptsystem (3)

طاهرا لجمل یو مصري عالم دی. هغه په Cryptography (1985) کي یوه نوي طریقه پیدا کړه چه د Elgamal-Cryptsystem په نوم یادیږي.

الجمل د Cryptsystem لپاره دیو دوراني ګروپ G څخه استفاده کوي :

$$G =< g >, ord(G) = n$$

مونږ پیغام استوونکی کس په S اوپیغام اخیستونکي په R سره ښيو.

R کیلي ګاني په لاندي شکل جوړوي:

یو $a \in \{2,3, \ldots, n-1\}$ انتخابوي او $A := g^a$ وضع کوي

a : private key (1)

$(G =< g >, A)$:public key (2)

بیا R ددي public key (عمومي کیلي) په باره S ته معلومات ورکوي

د S پیغام استوونکی وظیفه:

یو عنصر $m \in G$ د پیغام په حیث او یو عدد $b \in \{2,3, \ldots, n-1\}$ انتخابوي.

بیا $C := A^b . m$ ، $B := g^b$ وضع کوي او (B, C) پیغام اخیستونکي R ته لیږي.

اوس R هغه رمزی پیغام په m اصلی پیغام په لاندي ډول بدلوي:

$$B^{-a}.C = g^{-ab}\,A^{b}.m = (g^{-a})^{b}.A^{b}.m = A^{-b}.A^{b}.m = m$$

مثال: S غواړي یو پیغام دمثال په ډول د 4 عدد پیغام اخیستونکي ته ولیږي. لدي کارلپاره مونږد $(\mathbb{Z}^{*}{}_{7},.)$ دوراني ګروپ استعمالو.

$$G := (\mathbb{Z}^{*}{}_{7},.)\,, G =< g > = < \bar{3} >, ord(G) = 6$$

پیغام اخیستونکی:

private key : $a = 2 \in \{2,3,4,5\}$

$A := g^{a} = (\bar{3})^{2} = \bar{9} = \bar{7} + \bar{2} = \bar{2}$

public key: $(G =< g >, A) = (\bar{3},\bar{2})$

پیغام استوونکی:

4 د $(\mathbb{Z}^{*}{}_{7},.)$ د عنصر په شکل لیکي اوبیایي په رمزی پیغام بدلوي :

$m = \bar{4} \in G\ , b = 3 \in \{2,3,4,5\}$

$B = g^{b} = (\bar{3})^{3} = \overline{27} = \overline{21} + \bar{6} = \bar{6}$

$C = A^{b}.m = (\bar{2})^{3}.\bar{4} = \bar{8}.\bar{4} = \bar{1}.\bar{4} = \bar{4}$

$(B,C) = (\bar{6},\bar{4})$

اوس $(B,C) = (\bar{6},\bar{4})$ پیغام اخیستونکي ته لیږي

پیغام اخیستونکي:

$(B,C) = (\bar{6},\bar{4})$

R اصلي پیغام په لاندي ډول لاسته راوړي:

$$B^{-a}.C = (\bar{6})^{-2}.\bar{4} = \frac{1}{36}.\bar{4} = \frac{1}{1}.\bar{4} = \bar{4}$$

په نتیجه کي پوه شو چي اصلي پیغام 4 دی

مثال: پدي مثال کي احمد غواړي یوپیغام د "DE" په نامه قادر ته ولیږي.
پدي مثال کي د $(\mathbb{Z}^{*}{}_{11},.)$ دوراني ګروپ څخه استفاده کو

$$G := (\mathbb{Z}^{*}{}_{11},.)\,, G =< g > = < \bar{2} >, ord(G) = 10$$

پیغام اخیستونکی:

private key : $a = 3 \in \{2,3,4,5,6,7,8,9\}$

$A := g^{a} = (\bar{2})^{3} = \bar{8}$

public key: $(G =< g >, A) = (\bar{2},\bar{8})$

پیغام استونکی:

د جدول له مخي لاندي رابطي پیداکوي:

$D \leadsto 4\ , E \leadsto 5$

پورتني اعداد د $(\mathbb{Z}^*{}_{11},.)$ عنصرپه شکل ليکي اوبياهغه په عددي رمزی پيغام په لاندي ډول بدلوي:

$b = 2 \in \{2,3,4,5,6,7,8,9\}$
$B = g^b = (\bar{2})^2 = \bar{4}$
$m = 4$
$\bar{m} = \bar{4} \in (\mathbb{Z}^*{}_{11},.)$
$c_1 = A^b . \bar{m} = (\bar{8})^2 . \bar{4} = \overline{64} . \bar{4} = \bar{9} . \bar{4} = \bar{3}$

$m = 5$
$\bar{m} = \bar{5} \in (\mathbb{Z}^*{}_{11},.)$
$c_2 = A^b . \bar{m} = (\bar{8})^2 . \bar{5} = \overline{64} . \bar{5} = \bar{9} . \bar{5} = \bar{1}$
$C \coloneqq \{c_1, c_2\} = \{\bar{3}, \bar{1}\}$

اوس (B, C) پيغام اخيستونکي ته ليږي

پيغام اخيستونکي:

عددي اصلي پيغام په لاندي ډول لاسته راوړي:

$$B^{-a}. c_1 = (\bar{4})^{-3} . \bar{3} = \frac{1}{\overline{64}} . \bar{3} = \frac{1}{\bar{9}} . \bar{3} = \frac{1}{\bar{3}} = (\bar{3})^{-1} = \bar{4}$$
$$B^{-a}. c_2 = (\bar{4})^{-3} . \bar{1} = \frac{1}{\overline{64}} . \bar{1} = \frac{1}{\bar{9}} . \bar{1} = \frac{1}{\bar{9}} = (\bar{9})^{-1} = \bar{5}$$

دجدول له مخي:

په نتيجه کي قادر پيداکړ،چي راليږل شوی پيغام DE دي

تبصره: دلته په مثالونو کي د محاسبي داساني لپاره p ، q او $(\mathbb{Z}^*{}_n,.)$ کوچني انتخاب شويدي دي. څرنګه چه پيغامونه په عمومی صورت اوږده دي ، پس اعداد لوي انتخابيږي اومحاسبه يي د کمپيوتری پروګرامونو په واسطه په اسانی اجرا کيدای شي

تمرين: په **AFGHAN** پيغام باندي هغه دري کريپت سيستيم (Cryptsystem) تطبيق کړي

سمبولونه (Symbols)

$a := b$	a د b څخه تعریف شوی دی
$a \Rightarrow b$	د a افاده د b څخه لاس ته راځي
$a \Leftrightarrow b$	د a افادې څخه b اود b څخه a لاس ته راځي
$A = \emptyset$	A خالی سیت دی
$A \neq \emptyset$	A خالی سیت دی نه دی
$a \in A$	a یو عنصر په A سیت کې دی
$a \notin A$	a په A سیت کې شامل نه دی
$\forall a \in A$	هر a په A کې
$\wedge$	(conjuction)logical **and** (او)
	مثال $a \wedge b$: a **او** b افادي صدق کوي
$\vee$	(disjunction)logical **or** (یا)
	مثال $a \vee b$: د a **یا** د b افاده صدق کوي
$\neg$	not (negation) (متناقض)
$\cup$	د سیتونو اتحاد (union)
$\cap$	د سیتونو تقاطع (intersection)
$A \subset B$	A فرعی سیت (sub set) د B دی
$A \subseteq B$	A فرعی ست (sub set) د B اویا مساوی د B سره دی
$A \setminus B$	$\{ a \in A \mid a \notin B \}$
$\exists b \in A$	یو b عنصر د A په سیت کی موجود دی
$\nexists b \in A$	یو b عنصر د A په سیت کی جود نه لری
$\exists! b \in A$	فقط یوائې یو b د A په سیت کی موجود دی
$N \trianglelefteq G$	N نورمال په G کې

اختصارات او تشریحات

$\mathbb{N}$ د طبیعی اعدادو سیت

$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$

$\mathbb{Z}$ دپوره (تام) اعدادو سیت — $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$

$\mathbb{Q}$ د ناطق اعدادو سیت — $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$

$\mathbb{R}$ د حقیقی اعدادو سیت — $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$

$\mathbb{R}_+$ د مثبت حقیقی اعدادو سیت — $\mathbb{R}_+^* := \mathbb{R}_+ \setminus \{0\}$

$\mathbb{R}_+^0$ د مثبت حقیقی اعدادو سیت د صفرسره

$\mathbb{R}_-$ د منفی حقیقی اعدادو سیت — $\mathbb{R}_-^* := \mathbb{R}_- \setminus \{0\}$

$\mathbb{R}_-^0$ د منفی حقیقی اعدادو سیت د صفر سره

$\mathbb{C}$ د موهومي اویاد مختلط اعدادو سیت — $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$

Greek یونانی

homomorphism (Greek : homo same , morph form)

epimorphism (Greek: epi upon)

monomorphism (Greek: mono alone (یوازی))

isomorphism (Greek: iso equal

G-Hom گروپ هومومورفیزم (Group Homomorphism)

G-Monom گروپ مونومورفیزم (Group Homomorphism)

G-Epim گروپ ایپومورفیزم (Group Epimorphism)

G-End گروپ اندومورفیزم (Group Endomorphism)

G-Isom گروپ ایزومورفیزم Group Isomorphism)

G-Aut گروپ اوتومورفیزم (Group Automorphism)

R-Hom رینگ هومومورفیزم (Ring Homomorphism)

R-End رینگ اندومورفیزم (Ring Endomorphism)

R-Aut رینگ اوتومورفیزم (Ring Automorphism)

R-Isom رینگ ایزومورفیزم (Ring Isomorphism)

Greek Letters

[یونانی حرفونه]

Uppercase (لوی حرفونه)		lowercase (کوچنی حرفونه)		
Α	alpha	α		
Β	beta	β		
Γ	gamma	γ		
Δ	delta	δ		
Ε	epsilon	ε	ϵ	epsilon variant
Ζ	zeta	ζ		
Η	eta	η		
Θ	theta	θ	ϑ	theta variant
Ι	iota	ι		
Κ	kappsa	κ		
Λ	lambda	λ		
Μ	mu	μ		
Ν	nu	ν		
Ξ	xi	ξ		
Ο	onmicron	o		
Π	pi	π		
Ρ	rho	φ	ϱ	rho vaiant
Σ	sigma	σ	ς	sigma variant
Τ	tau	τ		
Υ	upsilon	υ		
Φ	phi	φ	ϕ	phi variant
Χ	chi	χ		
Ψ	psi	ψ		
Ω	omega	ω		

Bibliography

Prof.Dr. Meyberg Algebra(gruppen,ringen,korper)2008
Van der waerden Algebra 1 1993
G.Ficher Lehrbuch der algebra 2008
D.A.R Wallace Groups, Rings und fields 2001
Chr.Nelius Grundlage der algebra Vorlesung 2005
S. Busch Algebra 1999
M. Junker Gruppentheorie vorlesung 2002
M. Ziegler Einfürung in die Algebra Vorlesung 1999/ 2000
Chr.nelius Grundlage der Algebra Vorlesung 2005
Prof. Dr. A. Werner Algebra I Vorlesung WS 2004/2005
Prof. Dr. H. Brenner Einführung in die Algebra Vorlesung SS 2009
Prof. Zink Algebra I WS 2005/20046

دليکوال ځان پيژندنه

ځه د بلخ ولسوالی د مهمندانوپه کلي زيږيدلی يم. د مهمندانود لمړی ښونځی د فارغيدو وروسته د کابل دابن سينا په منځنی ښونځی کی شامل شوم.
د دارالمعليمين دفارغيدومی وروسته څوکاله مي دښونکی دنده درلوده. کابل د ساينس پوهنځی د فارغيدووروسته هلته د رياضی په ديپارتمنت کی په علمی کادرکی وگمارل شوم. په هغه وخت کی د کابل پوهنتون د ساينس پوهنځی او د المان فدرالی دولت د Rheinischen Friedrich Wilhelms Univesity ترمينځ تواميت موجود وه. په همدي اساس ماته بورس راکړل شواوځه درياضې په څانگه کي د لوړوزدکولپاره المان ته ولاړم. هلته می لمړی ديپلوم اووروسته مې ډاکترۍ درياضی په څانگه کي د Bonn ښار په پورتنی پوهنتون کی لاسته راوړه.
د 2009 کاله راهيسی دهرات اوننگرهارپه پوهنتونوکی مې څوسميستره دخطي اومعاصر الجبر تدريس کړيدی. ديادشوي مضمونوپه برخه کي مي په پشتواودري ژبوليکني هم کړيدي

Contents

Publishing Textbooks

Honorable lecturers and dear students**!**

The lack of quality textbooks in the universities of Afghanistan is a serious issue, which is repeatedly challenging students and teachers alike. To tackle this issue, we have initiated the process of providing textbooks to the students of medicine. For this reason, we have published Nearly 300 different textbooks of Medicine, Engineering, Science, Economics, Journalism and Agriculture (96 medical textbooks funded by German Academic Exchange Service, 170 medical and non-medical textbooks funded by German Aid for Afghan Children, 7 textbooks funded by German-Afghan University Society, 2 textbooks funded by Consulate General of the Federal Republic of Germany, Mazar-e Sharif, 3 textbooks funded by Afghanistan-Schulen, 2 textbooks funded by SlovakAid, 1 textbook funded by SAFI Foundation and 8 textbooks funded by Konrad Adenauer Stiftung) from Nangarhar, Khost, Kandahar, Herat, Balkh, Al-Beroni, Kabul, Kabul Polytechnic and Kabul Medical universities. The book you are holding in your hands is a sample of a printed textbook. It should be mentioned that all these books have been distributed among all Afghan universities and many other institutions and organizations for free. All the published textbooks can be downloaded from www.ecampus-afghanistan.org.

The Afghan National Higher Education Strategy (2010-2014) states**:**

"Funds will be made available to encourage the writing and publication of textbooks in Dari and Pashto. Especially in priority areas, to improve the quality of teaching and learning and give students access to state–of–the–art information. In the meantime, translation of English language textbooks and journals into Dari and Pashto is a major challenge for curriculum reform. Without this facility it would not be possible for university students and faculty to access modern developments as knowledge in all disciplines accumulates at a rapid and exponential pace, in particular this is a huge obstacle for establishing a research culture. The Ministry of Higher Education together with the universities will examine strategies to overcome this deficit **".**

We would like to continue this project and to end the method of manual notes and papers. Based on the request of higher education institutions, there is the need to publish about 100 different textbooks each year.

I would like to ask all the lecturers to write new textbooks, translate or revise their lecture notes or written books and share them with us to be published. We will ensure quality composition, printing and distribution to Afghan universities free of charge. I would like the students to encourage and assist their lecturers in this regard. We welcome any recommendations and suggestions for improvement.

It is worth mentioning that the authors and publishers tried to prepare the books according to the international standards, but if there is any problem in the book, we kindly request the readers to send their comments to us or the authors in order to be corrected for future revised editions.

This Publication was funded by Inasys GmbH in Germany.
I am especially grateful to GIZ (German Society for International Cooperation) and CIM (Centre for International Migration & Development) for providing working opportunities for me from 2010 to 2016 in Afghanistan.
In our ministry, I would like to cordially thank to Deputy minister of Academic Affaires & Acting Minister of Higher Education Prof Abdul Tawab Balakarzai, Administrative & Financial Deputy Minister Prof Dr. Ahmad Seyer Mahjoor (PhD), Administrative & Financial Director Ahmad Tariq Sediqi, Advisor at Ministry of Higher Education Dr. Gul Rahim Safi, Chancellor of Universities, Deans of faculties, and lecturers for their continuous cooperation and support for this project .
I am also thankful to all those lecturers who encouraged us and gave us all these books to be published and distributed all over Afghanistan. Finally I would like to express my appreciation for the efforts of my colleagues Hekmatullah Aziz and Fahim Habibi in the office for publishing books.

Dr Yahya Wardak
Advisor at the Ministry of Higher Education
Kabul, Afghanistan, November, 2019
Office: 0756014640, 0706320944
Email: textbooks@afghanic.de

Message from the Ministry of Higher Education

In history, books have played a very important role in gaining, keeping and spreading knowledge and science, and they are the fundamental units of educational curriculum which can also play an effective role in improving the quality of higher education. Therefore, keeping in mind the needs of the society and today's requirements and based on educational standards, new learning materials and textbooks should be provided and published for the students.

I appreciate the efforts of the lecturers and authors, and I am very thankful to those who have worked for many years and have written or translated textbooks in their fields. They have offered their national duty, and they have motivated the motor of improvement.

I also warmly welcome more lecturers to prepare and publish textbooks in their respective fields so that, after publication, they should be distributed among the students to take full advantage of them. This will be a good step in the improvement of the quality of higher education and educational process.

The Ministry of Higher Education has the responsibility to make available new and standard learning materials in different fields in order to better educate our students.

Finally I am very grateful to our colleague Dr. Yahya Wardak that have provided opportunities for publishing this book.

I am hopeful that this project should be continued and increased in order to have at least one standard textbook for each subject, in the near future.

Sincerely,
Prof Abdul Tawab Balakarzai
Deputy Minister of Academic Affairs &
Acting Minister of Higher Education
Kabul, 2019

Book Name Algebra (in Pashto)

Author Dr Abdullah Mohmand

Publisher Shaikh Zayed University, Science Faculty

Website www.szu.edu.af

Published 2019, First Edition

Copies 1000

Serial No 293

Download www.ecampus-afghanistan.org

This Publication was funded by inasys GmbH in Germany and Administrative and technical support by Afghanic.

The contents and textual structure of this book have been developed by concerning author and relevant faculty and being responsible for it. Funding and supporting agencies are not holding any responsibilities.

If you want to publish your textbooks, please contact us:

Dr. Yahya Wardak, Ministry of Higher Education, Kabul

Office 0756014640, 0706320844

Email textbooks@afghanic.de

Printed in Afghanistan 2019

Sahar Printing Press

ISBN 978-9936-620-67-4